

Rec'd PCT/TO 31 AUG 2004

特許協力条約に基づいて公開された国際出願

505,174  
10/505174

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2004年7月29日 (29.07.2004)

PCT

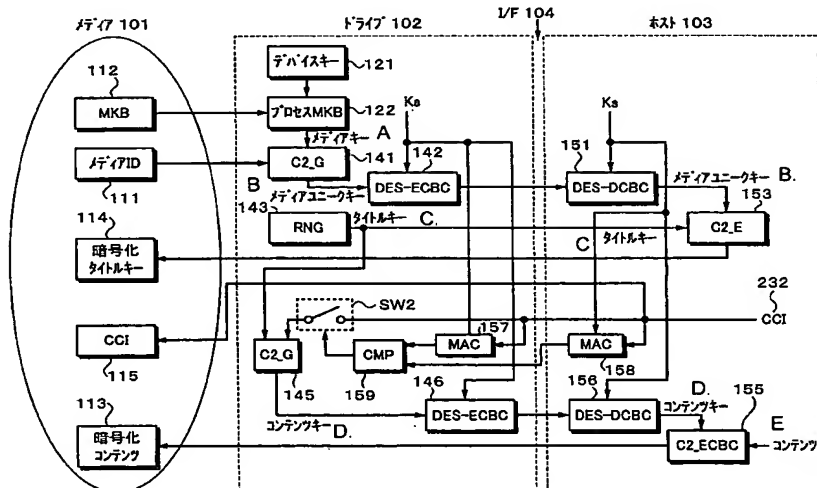
(10) 国際公開番号  
WO 2004/064314 A1

- (51) 国際特許分類<sup>7</sup>: H04L 9/10, G11B 20/10, 20/12
- (21) 国際出願番号: PCT/JP2003/016937
- (22) 国際出願日: 2003年12月26日 (26.12.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願2003-006916 2003年1月15日 (15.01.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
- (73) 発明者/出願人 (米国についてのみ): 木谷 聡 (KI-TANI, Satoshi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 村松 克美 (MURAMATSU, Katsumi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 杉浦 正知, 外 (SUGIURA, Masatomo et al.); 〒171-0022 東京都豊島区南池袋2丁目49番7号 池袋パークビル7階 Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,

[続葉有]

(54) Title: SIGNAL PROCESSING SYSTEM, RECORDING METHOD, PROGRAM, RECORDING MEDIUM, REPRODUCTION DEVICE, AND INFORMATION PROCESSING DEVICE

(54) 発明の名称: 信号処理システム



101...MEDIUM  
111...MEDIUM ID  
114...ENCRYPTION TITLE KEY  
113...ENCRYPTED CONTENT  
102...DRIVE  
121...DEVICE KEY  
122...PROCESS MKB  
A...MEDIUM KEY  
B...MEDIUM UNIQUE KEY  
C...TITLE KEY  
D...CONTENT KEY  
103...HOST  
E...CONTENT

(57) Abstract: A recorder consists of a drive (102) and a host (103) performing mutual authentication. C2\_G (141) of the drive (102) is transferred to the host (103) after a medium unique key calculated by the medium ID and a medium key is encrypted by using a session key (Ks) generated by mutual authentication. A title key generated by a random number generator (143) of the drive (102) is transferred to the host (103). C2\_G (145) of the drive (102) is transferred to the host (103) after the content key calculated from the title key and the CCI (232) is encrypted by using the session key (Ks). By using the content key decrypted by the host (103), the content is encrypted and the drive (102) records the encrypted content, encryption title key, and the CCI (232) onto a medium (101).

(57) 要約: 相互認証を行うドライブ102とホスト103とからレコーダが構成される。ドライブ102のC2\_G141がメディアIDとメディアキーから計算したメディアユニークキーが相互認証によって生成したセッションキーKsを用いて暗号化されてからホスト103に転送される。

[続葉有]

WO 2004/064314 A1



LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

- (84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

ドライブ 102 の乱数発生器 143 が発生したタイトルキーがホスト 103 に転送される。ドライブ 102 の C2 G145 がタイトルキーと CC1232 とから計算したコンテンツキーがセッションキー Ks を用いて暗号化されてからホスト 103 へ転送される。ホスト 103 が復号したコンテンツキーを用いてコンテンツを暗号化し、ドライブ 102 が暗号化コンテンツ、暗号化タイトルキーおよび CC1232 をメディア 101 へ記録する。

## 明 細 書

## 信号処理システム

5

## 技術分野

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される信号

10 処理システム、記録方法、プログラム、記録媒体、再生装置および情報処理装置に関する。

## 背景技術

近年開発されたDVD (Digital Versatile Disc)等の記録媒体では

15 、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

DVD-Videoでは、コピープロテクション技術としてCSS (Content Scrambling System) が採用されている。CSSは、DVD-ROMメディアに対する適用のみが認可されており、DVD-R、DVD-RW、DVD+R、DVD+RW等の記録型DVDでのCSSの利用がCSS契約によって禁止されている。したがって、CSS方式で著作権保護されたDVD-Videoの内容を記録型DVDへのま

20 とコピー（ビットバイビットコピー）することは、CSS契約上では、認められた行為ではない。

25

しかしながら、C S S の暗号方式が破られる事態が発生した。C S S の暗号化を解除してD V D -Video の内容を簡単にハードディスクにコピーすることを可能とする「D e C S S」と呼ばれるソフトウェアがインターネット上で配布された。「D e C S S」が出現した背景  
5 には、本来耐タンパー化が義務付けられているはずのC S S復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にC S Sアルゴリズム全体が解読された経緯がある。

C S Sの後に、D V D -Audio等のD V D -R O Mの著作権保護技術であるC P P M (Content Protection for Pre-Recorded Media)、  
10 並びに記録型D V D、メモリカードに関する著作権保護技術C P R M (Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、データをまるごとコピーしても再生  
15 を制限できる特徴を有している。D V Dに関する著作権保護の方法に関しては、下記の非特許文献1に説明され、C P R Mは、ライセンス管理者である米4C Entity, LLC が配布する下記の資料に説明されている。

山田, 「D V Dを起点に著作権保護空間を広げる」, 日経エレクトロ  
20 ニクス 2001.8.13, p.143-153

"Content Protection for Recordable Media Specification DVD Book", インターネット<URL : <http://www.4Centity.com/>>

パーソナルコンピュータ(以下、適宜P Cと略す)環境下では、P Cとドライブとが標準的インターフェースで接続されるために、標準  
25 的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。アプリケーションソフトウェア

がリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

著作権保護技術をP C上で実行されるアプリケーションプログラム  
5 へ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がない。その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。C S Sの場合は、結果としてその著作権保  
10 護技術が破られてしまった。C S Sの後に提案されたC P P Mおよび記録型D V Dに関する著作権保護技術C P R Mにおいても、既に破られているC S Sに新たな機能を加えたものであり、また、著作権保護技術に関わるアルゴリズムは、大部分がP Cでの実装に依存するものであり、コンテンツプロテクションの機能が十分に強いものと言えな  
15 い問題があった。すなわち、アプリケーションソフトウェアなどのリバースエンジニアリングによって、著作権保護技術に関わる秘密情報の解析により暗号方式が破られ、ディスクからのデータとしてP Cがそのまま読み出した暗号化コンテンツが「D e C S S」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとして  
20 てコピー制限の働かない状態で複製が繰り返されるような事態を招くことで、著作権保護が機能しなくなるという危険性があった。

この発明の目的は、P C環境下でも著作権保護技術の安全性を確保することができる相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置を提供することにある。

25

発明の開示

上述した課題を解決するために、この発明の第 1 の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達部を介して相互認証接続される情報処理装置とを備える信号処理システムであって、

- 5     再生装置は、  
中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、  
中間鍵情報を伝達部を介して情報処理装置へ送る第 1 の送信部と、  
コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第 2

- 10    の送信部とを有し、  
情報処理装置は、  
コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、

- 記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化部と、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録部とを有する信号処理システムである。

- この発明の第 2 の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達部を介して  
20    相互認証接続される情報処理装置とが、記録媒体に情報を記録する記録方法であって、

再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

- 25    中間鍵情報を伝達部を介して情報処理装置へ送る第 1 の送信ステップと、

- コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第 2  
の送信ステップとを有し、  
情報処理装置は、  
コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテ  
5   ンツ情報暗号化ステップと、  
記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を  
用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、  
暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記  
録媒体に記録する記録ステップとを有する記録方法である。
- 10   この発明の第 3 の態様は、記録媒体固有の情報をあらかじめ備えた  
記録媒体から情報を読み出す再生装置と、再生装置が伝達部を介して  
相互認証接続される情報処理装置とが、記録媒体に情報を記録するプ  
ログラムであって、  
再生装置に、
- 15   中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号  
化鍵生成ステップと、  
中間鍵情報を伝達部を介して情報処理装置へ送る第 1 の送信ステッ  
プと、  
コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第 2  
20   の送信ステップとを行わせ、  
情報処理装置に、  
コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテ  
ンツ情報暗号化ステップと、  
記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を  
25   用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、  
暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記

録媒体に記録する記録ステップとを行わせるプログラムである。

この発明の第 4 の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達部を介して相互認証接続される情報処理装置とが、記録媒体に情報を記録するプログラムを格納した記録媒体であって、

再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達部を介して情報処理装置へ送る第 1 の送信ステップと、

コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第 2 の送信ステップを行わせ、

情報処理装置に、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを行わせるプログラムを格納した記録媒体である。

この発明の第 5 の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出し、伝達部を介して情報処理装置と接続される再生装置であって、中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、

中間鍵情報を伝達部を介して情報処理装置へ送る第 1 の送信部と、コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第 2



の送信部とを有し、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化部と、暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録部とを有する情報処理装置と相互認証接続される再生装置である。

この発明の第 6 の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と伝達部を介して接続される情報処理装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、中間鍵情報を伝達部を介して情報処理装置へ送る第 1 の送信部と、コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第 2 の送信部とを有する再生装置と伝達部を介して相互認証接続され、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化部と、

暗号化されたコンテンツ情報および暗号化された中間鍵情報を記録媒体に記録する記録部とを有する情報処理装置である。

この発明の第 7 の態様は、不正な電子機器を無効化するための第 1 の情報と、コンテンツ毎に異なる第 2 の情報と、暗号化単位毎に定義可能な第 3 の情報と、スタンパ毎に異なる識別データとが記録された記録媒体へ暗号化されたデータを記録する記録部および記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方

と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 4 の情報が格納される格納部と、

- 5     第 1 の情報と第 4 の情報とから当該格納された第 4 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であることを判定するリボーク処理部と、

- リボーク処理部で第 4 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であると判定された場合に、第 1 の情報  
10   、第 4 の情報、第 2 の情報および識別データから、個々の記録媒体毎に固有の中間鍵情報を求める演算部と、

中間鍵情報を伝達部を介して情報処理装置の最終暗号化鍵生成部へ送る送信部とを有する再生装置である。

- この発明の第 8 の態様は、正当な電子機器またはアプリケーション  
15   ソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 4 の情報を有するとともに、不正な電子機器を無効化するための第 1 の情報と、コンテンツ毎に異なる第 2 の情報と、暗号化単位毎に定義可能な第 3 の情報と、スタンパ毎に異なる識別データとが記録された記録媒体への暗号化されたデータの記録および  
20   記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置との認証を行う認証部と、

- 記録再生装置から、認証が成立した場合に形成されるセッションキーによって暗号化された、第 1 の情報、第 4 の情報、第 2 の情報および識別データから生成された個々の記録媒体毎に固有の中間鍵情報を  
25   受け取り、当該中間鍵情報を復号する鍵情報復号部と、

記録再生装置から受け取った第 3 の情報と、復号された中間鍵情報

から最終暗号化鍵を生成する最終暗号化鍵生成部と、

最終暗号化鍵による暗号化と最終暗号化鍵による復号との少なくとも一方を行う暗号化復号部とを有するデータ処理装置である。

この発明では、再生装置側でコンテンツキーを生成し、情報処理装置側でコンテンツキーによってコンテンツを暗号化している。このように著作権保護のための鍵情報の生成を再生装置で行うので、ハードウェア構成でコンテンツキーを生成することが可能となり、耐タンパ性を高めることができる。また、再生装置において、乱数を生成し、乱数を中間鍵とするので、再生装置において、真正乱数またはそれに近い乱数をハードウェア例えばLSIによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。このように、この発明では、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

この発明では、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばLSIによって生成できるので、PC内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる等のおそれを少なくできる。

25

図面の簡単な説明

第 1 図は、先に提案されているレコーダ、プレーヤおよび D V D メディアからなるシステムを説明するためのブロック図である。

第 2 図は、P C ベースの D V D メディア記録再生システムを説明するためのブロック図である。

- 5 第 3 図は、第 2 図のシステムにおける D V D ドライブ 4 およびホスト 5 の処理の手順を説明するための略線図である。

第 4 図は、第 2 図のシステムにおける認証動作を説明するためのフローチャートである。

- 10 第 5 図は、この発明の一実施形態による相互認証のための構成を示すブロック図である。

第 6 図は、この発明の一実施形態におけるドライブの認証動作の処理の手順を説明するためのフローチャートである。

第 7 図は、この発明の一実施形態におけるホストの認証動作の処理の手順を説明するためのフローチャートである。

- 15 第 8 図は、この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の一例を示すブロック図である。

第 9 図は、レコーダの一例の通信の手順を説明するための略線図である。

- 20 第 1 0 図は、この発明の一実施形態によるドライブとホストを組み合わせたプレーヤの構成の一例を示すブロック図である。

第 1 1 図は、プレーヤの一例の通信の手順を説明するための略線図である。

第 1 2 図は、この発明の他の実施形態によるドライブとホストを組み合わせたレコーダの構成の一例を示すブロック図である。

- 25 第 1 3 図は、この発明の他の実施形態によるドライブとホストを組み合わせたプレーヤの構成の一例を示すブロック図である。

## 発明を実施するための最良の形態

この発明の一実施形態の説明に先立って、特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

5    以下に説明する。

記録媒体：メディア例えばディスク、再生装置：ドライブ、情報処理装置：ホスト、伝達手段：ドライバ－ホストインターフェース、信号処理システム：メディアを再生するドライブとホストとがドライバ－ホストインターフェースを介して接続されるシステムである。第1  
10    の送信手段：ドライブ側からセッションキーを共通鍵とした共通鍵暗号方式で情報をホスト側に送る手段、第2の送信手段：逆にホスト側からセッションキーを共通鍵として情報をドライブ側に送る手段のことである。

コンテンツ情報：メディアに記録されている情報または記録すべき  
15    情報をコンテンツ情報としている。記録媒体固有の情報：メディアIDである。乱数を生成する乱数生成手段：乱数発生器（RNG：Random Number Generator）である。記録媒体固有の鍵情報：メディアユニークキー、中間鍵情報：タイトルキーである。コンテンツ情報暗号化鍵：コンテンツキー（記録時に使われるコンテンツキーをコンテンツ  
20    情報暗号化鍵とし、再生時に使われるコンテンツキーをコンテンツ情報復号鍵としている。）

この発明の理解の容易のために、最初に第1図を参照して著作権保護技術例えばDVD用CPRMのアーキテクチャについて説明する。  
第1図において、参照符号1が例えばCPRM規格に準拠したDVD  
25    －R/RW、DVD－RAM等の記録型DVDメディアを示す。参照符号2が例えばCPRM規格に準拠したレコーダを示す。参照符号3

が例えばC P R M規格に準拠したプレーヤを示す。レコーダ 2 およびプレーヤ 3 は、機器またはアプリケーションソフトウェアである。

未記録ディスクの状態において、D V Dメディア 1 の最内周側のリードインエリアのB C A (Burst Cutting Area)またはN B C A (Narrow Burst Cutting Area) と称されるエリアには、メディア I D 1 1 が記録されている。リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、M K B と適宜略す） 1 2 が予め記録されている。メディア I D 1 1 は、個々のメディア単位例えばディスク 1 枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディア I D 1 1 は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロック M K B は、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディア I D およびメディアキーブロックは、記録媒体固有の第 1 の情報である。

ディスク 1 の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ 1 3 が記録される。暗号化方式としては、C 2 (Cryptomeria Cipherring) が使用される。

D V Dメディア 1 には、暗号化タイトルキー 1 4 およびC C I (Copy Control Information) 1 5 が記録される。暗号化タイトルキー 1 4 は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。C C I は、コピーノーモア、コピーワンス、コピーフリー等のコピー制御情報である。

レコーダ 2 は、デバイスキー 2 1、プロセスM K B 2 2、C 2 \_\_ G 2 3、乱数発生器 2 4、C 2 \_\_ E 2 5、C 2 \_\_ G 2 6 およびC 2 \_\_ E C B C 2 7 の構成要素を有する。プレーヤ 3 は、デバイスキー 3 1、

プロセスMKB 3 2、C 2 \_\_G 3 3、C 2 \_\_D 3 5、C 2 \_\_G 3 6 およびC 2 \_\_D C B C 3 7の構成要素を有する。C 2 \_\_G 2 3および3 3は、それぞれメディアIDとメディアキーとからメディアユニークキーを演算するブロックである。C 2 \_\_G 2 6および3 6は、それぞれCCIとタイトルキーとからコンテンツキーを演算するブロックである。

デバイスキー2 1、3 1は、個々の装置メーカー、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。DVDメディア1から再生されたMKB 1 2とデバイスキー2 1とがプロセスMKB 2 2において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ2におけるのと同様に、プレーヤ3においても、MKB 1 2とデバイスキー3 1とがプロセスMKB 3 2において演算され、リボケーションされたかどうかの判別がなされる。

プロセスMKB 2 2、3 2のそれぞれにおいて、MKB 1 2とデバイスキー2 1、3 1からメディアキーが算出される。MKB 1 2の中にレコーダ2またはプレーヤ3のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ2またはプレーヤ3が正当なものではないと判断される。すなわち、そのようなレコーダ2またはプレーヤ3がリボケーションされる。

C 2 \_\_G 2 3、3 3は、それぞれ、メディアキーとメディアIDとを演算し、メディアユニークキーを導出する処理である。

乱数発生器(RNG: Random Number Generator) 2 4は、タイトル

キーの生成に利用される。乱数発生器 2 4 からのタイトルキーが C 2  
\_\_E 2 5 に入力され、タイトルキーがメディアユニークキーで暗号化  
される。暗号化タイトルキー 1 4 が DVD メディア 1 に記録される。

プレーヤ 3 では、DVD メディア 1 から再生された暗号化タイトル  
5 キー 1 4 とメディアユニークキーとが C 2 \_\_D 3 5 に供給され、暗号  
化タイトルキーがメディアユニークキーで復号され、タイトルキーが  
得られる。

レコーダ 2 においては、CCI とタイトルキーとが C 2 \_\_G 2 6 に  
供給され、コンテンツキーが導出される。コンテンツキーが C 2 \_\_E  
10 C B C 2 7 に供給され、コンテンツキーを鍵としてコンテンツが暗号  
化される。暗号化コンテンツ 1 3 が DVD メディア 1 に記録される。

プレーヤ 3 においては、CCI とタイトルキーとが C 2 \_\_G 3 6 に  
供給され、コンテンツキーが導出される。コンテンツキーが C 2 \_\_E  
C B C 3 7 に供給され、DVD メディア 1 から再生された暗号化コン  
15 テンツ 1 3 がコンテンツキーを鍵として復号される。

第 1 図の構成において、レコーダ 2 による記録の手順について説明  
する。レコーダ 2 は、DVD メディア 1 から MKB 1 2 を読み出し、  
プロセス MKB 2 2 によってデバイスキー 2 1 と MKB 1 2 とを演算  
し、メディアキーを計算する。演算結果が予め定められた値を示すな  
20 らば、デバイスキー 2 1 (レコーダ 2 の機器またはアプリケーション  
) が MKB によってリボークされたと判定される。レコーダ 2 は、以  
後の処理を中断し、DVD メディア 1 への記録を禁止する。若し、メ  
ディアキーの値が予め定められた値以外であれば、処理を継続する。

レコーダ 2 は、DVD メディア 1 からメディア ID 1 1 を読み、メ  
25 ディアキーと共にメディア ID を C 2 \_\_G 2 3 に入力しメディア毎に  
異なるメディアユニークキーが演算される。乱数発生器 2 4 で発生さ



せたタイトルキーがC 2 \_\_ E 2 5で暗号化され、暗号化タイトルキー  
1 4としてDVDメディア1に記録される。タイトルキーとコンテン  
ツのCCI情報がC 2 \_\_ G 2 6で演算され、コンテンツキーが導出さ  
れる。コンテンツキーでコンテンツをC 2 \_\_ E C B C 2 7で暗号化し  
5、DVDメディア1上に暗号化コンテンツ13としてCCI 1 5と共に  
記録する。

プレーヤ3による再生の手順について説明する。最初にM K B 1 2  
をDVDメディア1から読み出す。デバイスキー31とM K B 1 2を  
演算し、リボケーションの確認がなされる。デバイスキー31、すな  
10 わち、プレーヤ3の機器またはアプリケーションがリボークされない  
場合には、メディアIDを使用してメディアユニークキーが演算され  
、読み出された暗号化タイトルキー14とメディアユニークキーから  
タイトルキーが演算される。タイトルキーとCCI 1 5とがC 2 \_\_ G  
3 6に入力され、コンテンツキーが導出される。コンテンツキーがC  
15 2 \_\_ D C B C 3 7に入力され、コンテンツキーを鍵として、DVDメ  
ディア1から再生された暗号化コンテンツ13に対してC 2 \_\_ D C B  
C 3 7の演算が施される。その結果、暗号化コンテンツ13が復号さ  
れる。

このように、コンテンツの復号に必要なコンテンツキーを得るため  
20 には、DVDメディアの1枚毎に異なるメディアIDが必要となるの  
で、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコ  
ピーされても、他のメディアのメディアIDがオリジナルのメディア  
IDと異なるために、コピーされたコンテンツを復号することができ  
ず、コンテンツの著作権を保護することができる。

25 上述した第1図の構成は、記録再生機器として構成されたものであ  
る。この発明は、DVDメディア1に対するコンテンツ保護処理をP

C環境下で扱う場合に適用される。第2図を参照して現行の方式によるPCとドライブの役割分担を示す。第2図において、参照符号4が上述したCPRM規格に準拠したDVDメディア1を記録および再生する記録再生装置としてのDVDドライブを示す。

- 5 参照符号5がデータ処理装置としてのホスト例えばPCを示す。ホスト5は、DVDメディア1に記録可能で、DVDメディア1から再生可能なコンテンツを扱うことができ、且つDVDドライブ4と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばPCに対してアプリケーションソフトウェアがインストールされることによってホスト5が構成される。

DVDドライブ4とホスト5との間がインターフェース4aで接続されている。インターフェース4aは、ATAPI (AT Attachment with Packet Interface) , SCSI (Small Computer System Interface) , USB (Universal Serial Bus) , IEEE (Institute of Electrical and Electronics Engineers) 1394等である。

- DVDメディア1には、メディアID11、メディアキープロック12およびACC (Authentication Control Code) が予め記録されている。ACCは、DVDドライブ4とホスト5との間の認証がDVDメディア1によって異なるようにするために予めDVDメディア1に記録されたデータである。

DVDドライブ4は、ACC16をDVDメディア1から読み出す。DVDメディア1から読み出されたACC16がDVDドライブ4のAKE (Authentication and Key Exchange) 41に入力されると共に、ホスト5へ転送される。ホスト5は、受け取ったACCをAKE51に入力する。AKE41および51は、乱数データを交換し、この交換した乱数とACCの値とから認証動作の度に異なる値となる共

通のセッションキー（第2図の構成においてはバスキーと称する）を生成する。

バスキーがMAC (Message Authentication Code) 演算ブロック42および52にそれぞれ供給される。MAC演算ブロック42および52は、AKE41および51でそれぞれ得られたバスキーをパラメータとして、メディアIDおよびメディアキーブロック12のMACを計算するプロセスである。MKBとメディアIDの完全性(integrity)をホスト5が確認するために利用される。

MAC42および52によってそれぞれ計算されたMACがホスト5の比較53において比較され、両者の値が一致するかどうか判定される。これらのMACの値が一致すれば、MKBとメディアIDの完全性が確認されたことになる。比較出力でスイッチSW1が制御される。

スイッチSW1は、DVDドライブ4のDVDメディア1の記録または再生経路と、ホスト5の暗号化／（または）復号モジュール54との間の信号路をON/OFFするものとして示されている。スイッチSW1は、信号路のON/OFFを行うものとして示されているが、より実際には、ONの場合にホスト5の処理が継続し、OFFの場合にホスト5の処理が停止することを表している。暗号化／復号モジュール54は、メディアユニークキーと暗号化タイトルキーとCCIとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ13へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ13を復号する演算ブロックである。

メディアユニークキー演算ブロック55は、MKB12とメディアIDとデバイスキー56とからメディアユニークキーを演算する演算ブロックである。第1図に示すレコーダまたはプレーヤと同様に、デ

バイスキーとMKB 1 2 とからメディアキーが演算される。メディアキーとメディアID 1 1 とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リポー  
5 クされる。したがって、メディアユニークキー演算ブロック 5 5 は、リボケーションを行うリボーク処理部としての機能も有する。

記録時に、比較 5 3 によって完全性が確認された場合には、スイッチSW 1 がONされる。暗号化／復号モジュール 5 4 からスイッチSW 1 を通じてドライブ 4 に対して、暗号化コンテンツ 1 3、暗号化タイトルキー 1 4 およびCCI 1 5 が供給され、DVDメディア 1 に対してそれぞれ記録される。再生時に、比較 5 3 によって完全性が確認された場合には、スイッチSW 1 がONされる。DVDメディア 1 からそれぞれ再生された暗号化コンテンツ 1 3、暗号化タイトルキー 1 4 およびCCI 1 5 がスイッチSW 1 を通じてホスト 5 の暗号化／復  
10 号モジュール 5 4 に対して供給され、暗号化コンテンツが復号される。  
15

第 3 図は、第 2 図に示す現行のPC環境下のDVDメディアを利用するシステムにおいて、DVDメディア 1 と、DVDドライブ 4 と、ホスト 5 との間の信号の授受の手順を示す。ホスト 5 がDVDドライブ 4 に対してコマンドを送り、DVDドライブ 4 がコマンドに  
20 応答した動作を行う。

ホスト 5 からの要求に応じてDVDメディア 1 上のACCがシークされ、読み出される（ステップS 1）。次のステップS 2において、読み出されたACCがAKE 4 1 に入力されると共に、ホスト 5 へ転  
25 送され、ホスト 5 では、受け取ったACCがAKE 5 1 へ入力される。AKE 4 1 および 5 1 は、乱数データを交換し、この交換した乱数

とACC16の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをDVDドライブ4とホスト5が共有する。相互認証が成立しなかった場合では、処理が中断する。

認証動作は、電源のON後のディスク検出時並びにディスクの交換時には、必ず行われる。記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

認証が成功すると、ステップS3において、ホスト5がDVDドライブ4に対して、DVDメディア1からのMKB（メディアキーブロック）パック#0の読み出しを要求する。MKBは、パック0～パック15の16セクタが12回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

DVDドライブ4がステップS4においてMKBのパック#0を読みに行き、ステップS5において、パック#0が読み出される。DVDドライブ4は、モディファイドMKBをホスト5へ戻す（ステップS6）。MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を付加してホスト5へデータを転送する。パック#0以外の残りのMKBパックの要求と、DVDドライブ4の読み出し動作と、モディファイドMKBパックの転送動作とがMKBのパックがなくなるまで、例えばパック#15が読み出され、ホスト5へ転送されるまで、ステップS7およびS8によって繰り返される。

ホスト5がDVDドライブ4に対してメディアIDを要求する。DVDドライブ4がDVDメディア1に記録されているメディアIDを読みに行き、ステップS11において、メディアIDが読み出される

。DVDドライブ4は、メディアIDを読み出す際に、バスキーをパラメータとしてそのMAC値を計算する。DVDドライブ4はステップS12において、読み出されたメディアIDに対してMAC値m1を付加してホスト5へデータを転送する。

- 5     ホスト5では、DVDドライブ4から受け取ったMKB12およびメディアID11からバスキーをパラメータとして再度MAC値を計算し、計算したMAC値とDVDドライブ4から受け取ったMAC値とを比較53で比較する。両者が一致したならば、正しいMKBおよびメディアIDを受け取ったと判定して、スイッチSW1をONに設定して処理を先に進める。逆に両者が一致しなかったならば、MKBおよびメディアIDが改ざんされたものと判定して、スイッチSW1をOFFに設定して処理を中断する。
- 10

- ステップS13において、ホスト5がDVDドライブ4に対して暗号化コンテンツを要求し、ステップS14において、DVDドライブ
- 15     4が暗号化コンテンツを読み出し、ステップS13において、読み出した暗号化コンテンツがホスト5に転送される。ホスト5のメディアユニークキー演算ブロック55では、デバイスキー56とMKB12とメディアID11とによってメディアユニークキーが計算される。メディアユニークキーが暗号化／復号モジュール54に供給され、暗
- 20     号化タイトルキー14、CCI15からコンテンツキーが求められる。コンテンツキーを鍵としてDVDメディア1から読み出された暗号化コンテンツが復号される。DVDメディア1に対して記録されるコンテンツが暗号化される。

- 第4図のフローチャートにおいて、ステップST1は、MAC演算
- 25     ブロック42でバスキーをパラメータとして求められたMAC計算値と、MAC演算ブロック53でバスキーをパラメータとして求められ

たMAC計算値とを比較するステップである。両者が一致すれば、スイッチSW1がステップST2においてONとされる。両者が一致しない場合では、スイッチSW1がステップST3においてOFFとされ、処理が停止する。

- 5 上述したCPRMでは、DVD-Videoの著作権保護技術であるCSSと同じバスキー生成方法を採用している。CSS認証方式の内容は、本来秘密であるべき情報であるが、既に解析され一般ユーザーが入手可能なCSSライセンス管理団体であるDVD-CCAの許諾を得ていないフリーソフトウェアによって動作させることが可能となっている。
- 10 加えて、コンテンツプロテクション処理は、ホスト側でなされる、すなわち、リボケーション判定、メディアキー取得、メディアユニークキー導出、タイトルキー生成・導出からコンテンツキー導出およびコンテンツ暗号化・復号の全てがホスト側の処理であることから、著作権保護技術としての信頼性が低下している。
- 15 以下に述べるこの発明の一実施形態では、かかる問題点を解決するものである。一実施形態では、PC環境下でのコンテンツプロテクション処理におけるタイトルキー導出に関わる構成をドライブ内部に持ち、PCとの相互認証を経てタイトルキーおよびコンテンツキーをPCに送信するものである。
- 20 第5図は、一実施形態における相互認証の構成を示すブロック図であり、第6図は、ドライブ側の処理の流れを示すフローチャートであり、第7図は、ホスト側の処理の流れを示すフローチャートである。以下の説明において、参照符号101がメディア例えば光ディスクを示し、参照符号102がメディアのドライブを示し、参照符号103
- 25 がドライブ102とドライブーホストインターフェース104を介して接続されたホストを示す。メディア101は、上述したDVDメデ

5    ィアと同様の情報が予め記録されているものである。メディア 1 0 1  
は、記録可能なものに限らず、読み出し専用のものでも良い。ホスト  
1 0 3 がドライブ 1 0 2 に対して所定のコマンドを送り、その動作を  
制御する。使用するコマンドは、上述した非特許文献 2 に記載されて  
10    いるコマンド並びにコマンドを拡張したもの、および、メディア 1 0  
1 からコンテンツをセクタ・データとして読み出すための R E A D コ  
マンド、メディア 1 0 1 へコンテンツをセクタ・データとして書き込  
むための W R I T E コマンドである。

ドライブ 1 0 2 は、ドライブのデバイスキー 1 2 1 を有し、ホスト  
10    1 0 3 がホストのデバイスキー 1 3 1 を有している。デバイスキー 1  
2 1 は、多くの場合に L S I (Large Scale Integrated Circuit : 大  
規模集積回路) 内部に配置され、外部から読み出すことができないよ  
うセキュアに記憶される。デバイスキー 1 3 1 は、ソフトウェアプロ  
15    グラム内にセキュアに記憶される場合と、ハードウェアとしてセキュ  
アに記憶される場合とがある。ドライブ 1 0 2 がメディア 1 0 1 を扱  
う正当なドライブとなるためには、一実施形態のように、デバイスキ  
ーのような著作権保護技術に関する秘密情報を必要とするので、正規  
のライセンスを受けずに正規品になりすますようなクローン・ドライ  
ブの作成を防止できる効果がある。

20    第 5 図に示すように、ドライブ 1 0 2 には、M K B とデバイスキー  
1 2 1 とが入力され、ドライブのデバイスキーがリボケーションされ  
たかどうかを判定するプロセス M K B 1 2 2 が備えられている。ホス  
ト 1 0 3 にも同様に、プロセス M K B 1 3 2 が備えられている。リボ  
ケーションされない場合に、プロセス M K B 1 2 2 および 1 3 2 から  
25    それぞれメディアキー K m が出力される。リボーク判定処理がなされ  
、メディアキー K m が得られてから認証処理がなされる。



参照符号 1 2 3、1 2 4 および 1 2 5 は、メディアキー  $K_m$  をパラメータとして MAC 値を計算する MAC 演算ブロックをそれぞれ示す。参照符号 1 2 6、1 2 7 および 1 2 8 は、乱数発生器 (RNG: Random Number Generator) をそれぞれ示す。乱数発生器 1 2 6 が乱数 5 Ra1 を生成し、乱数発生器 1 2 7 が乱数 Ra2 を生成し、乱数発生器 1 2 8 が乱数 Ra3 を生成する。乱数発生器 1 2 6、1 2 7、1 2 8 は、例えば LSI の構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウェアとしても良いが、乱数 Ra1、  
10 Ra2、Ra3 は、互いに独立したものである。

ホスト 1 0 3 に、メディアキー  $K_m$  をパラメータとして MAC 値を計算する MAC 演算ブロック 1 3 3、1 3 4 および 1 3 5 と、乱数発生器 1 3 6、1 3 7 および 1 3 8 が備えられている。乱数発生器 1 3 6 が乱数 Rb1 を生成し、乱数発生器 1 3 7 が乱数 Rb2 を生成し、乱数  
15 発生器 1 3 8 が乱数 Rb3 を生成する。乱数発生器 1 3 6、1 3 7、1 3 8 は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

ドライブ 1 0 2 において生成された乱数とホスト 1 0 3 において生成された乱数とが交換される。すなわち、乱数 Ra1 および乱数 Rb1 が  
20 MAC 演算ブロック 1 2 3 および 1 3 3 に入力され、乱数 Ra2 および乱数 Rb2 が MAC 演算ブロック 1 2 4 および 1 3 4 に入力され、乱数 Ra3 および乱数 Rb3 が MAC 演算ブロック 1 2 5 および 1 3 5 に入力される。

ドライブ 1 0 2 の MAC 演算ブロック 1 2 3 が演算した MAC 値と  
25 、ホスト 1 0 3 の MAC 演算ブロック 1 3 3 が演算した MAC 値とがホスト 1 0 3 内の比較 1 3 9 において比較され、二つの値が同一か否

かが判定される。ここでのMAC値は、 $eK_m(Ra1 \parallel Rb1)$ と表記される。 $eK_m()$ は、メディアキー $K_m$ を鍵として括弧内のデータを暗号化することを表している。 $Ra1 \parallel Rb1$ の記号は、左側に乱数 $Ra1$ を配し、右側に乱数 $Rb1$ を配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、ホスト103によるドライブ102の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

ホスト103のMAC演算ブロック134が演算したMAC値と、ドライブ102のMAC演算ブロック124が演算したMAC値とがドライブ102内の比較129において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、 $eK_m(Rb2 \parallel Ra2)$ と表記される。比較の結果、二つの値が同一と判定されると、ドライブ102によるホスト103の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

かかる相互認証において、比較139および129の両者において、MAC値が同一と判定され、ドライブ102およびホスト103の両者の正当性が確認されると、すなわち、相互認証が成功すると、MAC演算ブロック125および135によって、共通のセッションキー $eK_m(Ra3 \parallel Rb3)$ がそれぞれ生成される。

さらに、上述した相互認証の処理の流れを第6図および第7図のフローチャートを参照して説明する。最初に、第7図のステップST20において、ホスト103がドライブ102に対して、コマンドREPORT KEYを発行し、MKBの転送を要求する。第6図のステップST10において、ドライブ102がメディア101からMKB112を読み出して、ホスト103へ転送する。

次に、ドライブ102がステップST11において、プロセスMK

B 1 2 2 によってメディアキー  $K_m$  を計算し、ホスト 1 0 3 がステップ S T 2 1 において、プロセス M K B 1 3 2 によってメディアキー  $K_m$  を計算する。この計算の過程でそれぞれが内蔵するデバイスキー 1 2 1 および 1 3 1 がリボケーションの対象とされているか否かが自分  
5 自身によって確認される（第 6 図中のステップ S T 1 2、第 7 図中のステップ S T 2 2）。

ドライブ 1 0 2 およびホスト 1 0 3 のそれぞれは、リボケーションの対象とされている場合にはリボークされ、処理が終了する。若し、ホスト 1 0 3 がリボケーションの対象とされていなければ、ステップ  
10 S T 2 3 において、コマンド SEND KEY により、ドライブ 1 0 2 に対して乱数発生器 1 3 6 および 1 3 7 でそれぞれ生成された乱数  $R_{b1}$  と乱数  $R_{b2}$  を転送する。若し、ドライブ 1 0 2 がリボケーションの対象とされていなければ、ステップ S T 1 3 において、ドライブ 1 0 2 がホスト 1 0 3 から転送されたこれらの乱数を受け取る。

15 その後、ホスト 1 0 3 は、コマンド REPORT KEY によりドライブ 1 0 2 に対してドライブ 1 0 2 が持つメディアキー  $K_m$  を鍵とした M A C によるレスポンス値と乱数生成器 1 2 6 が発生した乱数  $R_{a1}$  とをホスト 1 0 3 へ転送することを要求する（ステップ S T 2 4）。このレスポンス値は、 $eK_m(R_{a1} \parallel R_{b1})$  と表記される。 $eK_m()$  は、メディア  
20 キー  $K_m$  を暗号鍵として括弧内のデータを暗号化することを表している。 $R_{a1} \parallel R_{b1}$  の記号は、左側に乱数  $R_{a1}$  を配し、右側に乱数  $R_{b1}$  を配するように、二つの乱数を結合することを表している。

ホスト 1 0 3 からコマンド REPORT KEY を受け取ったドライブ 1 0 2 は、ステップ S T 1 4 において、M A C 演算ブロック 1 2 3 が生成した M A C 値  $eK_m(R_{a1} \parallel R_{b1})$  と乱数  $R_{a1}$  をホスト 1 0 3 へ転送する。ス  
25 テップ S T 2 5 において、ホスト 1 0 3 は、自身の M A C 演算プロッ

ク 1 3 3 で M A C 値を計算し、比較 1 3 9 においてドライブ 1 0 2 から受け取った値と一致するかの確認を行う。若し、受け取った M A C 値と計算された M A C 値とが一致したのなら、ホスト 1 0 3 によるドライブ 1 0 2 の認証が成功したことになる。ステップ S T 2 5 における比較の結果が同一でない場合には、ホスト 1 0 3 によるドライブ 1 0 2 の認証が失敗したことになり、リジェクト処理がなされる。

ホスト 1 0 3 によるドライブ 1 0 2 の認証が成功した場合には、ステップ S T 2 6 において、ホスト 1 0 3 がドライブ 1 0 2 へコマンド REPORT KEY を送付し、ドライブ 1 0 2 の乱数生成器 1 2 4 および 1 2 5 がそれぞれ生成する乱数 R a 2 と乱数 R a 3 の転送を要求する。このコマンドに応答して、ステップ S T 1 5 において、ドライブ 1 0 2 は、これらの乱数をホスト 1 0 3 へ転送する。

ステップ S T 2 7 において、ホスト 1 0 3 の M A C 演算ブロック 1 3 4 は、ドライブ 1 0 2 から受け取った乱数からホスト 1 0 3 が持つメディアキー K m を鍵とした M A C によるレスポンス値 e K m (R b 2 || R a 2 ) を計算し、乱数 R b 3 とともに、コマンド SEND KEY を用いてドライブ 1 0 2 へ転送する。

ステップ S T 1 6 において、ドライブ 1 0 2 は、ホスト 1 0 3 からレスポンス値 e K m (R b 2 || R a 2 ) および乱数 R b 3 を受け取ると、自身で M A C 値を計算し、ステップ S T 1 7 において、比較 1 2 9 によってホスト 1 0 3 から受け取った M A C 値と一致するかの確認を行う。若し、受け取った M A C 値と計算された M A C 値とが一致したのなら、ドライブ 1 0 2 によるホスト 1 0 3 の認証が成功したことになる。この場合には、ステップ S T 1 8 において、M A C 演算ブロック 1 2 5 がセッションキー e K m (R b 3 || R a 3 ) を生成し、ホスト 1 0 3 に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッション

ンキーは、認証動作の度に異なる値となる。

ステップ S T 1 7 における比較の結果が同一でない場合には、ドライブ 1 0 2 によるホスト 1 0 3 の認証が失敗したことになり、ステップ S T 1 9 において、認証が失敗したことを示すエラー情報がホスト 5 1 0 3 に送信される。

ホスト 1 0 3 は、送付したコマンド SEND KEY に対する応答としてドライブ 1 0 2 から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップ S T 2 8 において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップ S T 2 9 において、MAC 演算ブロック 1 3 5 がドライブ側と共通のセッションキー  $eK_m(Ra3 \parallel Rb3)$  (例えば 6 4 ビット長) を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。セッションキー 15  $eK_m(Ra3 \parallel Rb3)$  を以下の説明では、適宜  $K_s$  と表記する。

上述した一実施形態による相互認証は、ドライブ 1 0 2 がリボケーション機能を持つことができ、認証専用の特定の認証鍵を必要としない特徴を有している。

さらに、ドライブ 1 0 2 が比較 1 2 9 によってホスト 1 0 3 の認証 20 結果を確認することで、ドライブ 1 0 2 がホスト 1 0 3 から正規のライセンスを受けた上で実装されたものであるか否かを判定することが可能となる。

次に、上述した相互認証を行うドライブ 1 0 2 とホスト 1 0 3 とを組み合わせ実現したレコーダの一実施形態の構成を第 8 図に示す。 25 一実施形態のレコーダは、ドライブ 1 0 2 が計算したメディアユニークキーを相互認証によって生成したセッションキー  $K_s$  を用いてセキ

5 ュアにホスト 1 0 3 に転送する。また、ドライブ 1 0 2 の乱数発生器 1 4 3 によってタイトルキーが生成される。ドライブ 1 0 2 においてタイトルキーおよび C C I 2 3 2 からコンテンツキーが生成され、生成されたコンテンツキーがセッションキー K s を用いてホスト 1 0 3  
10 へセキュアに転送され、ホスト 1 0 3 が復号したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ 1 0 2 へ転送し、ドライブ 1 0 2 が暗号化コンテンツ、暗号化タイトルキーおよび C C I 2 3 2 をメディア 1 0 1 へ記録する構成とされている。メディア 1 0 1 に記録されている C C I に対して参照符号 1 1 5 を付す。

10 すなわち、ドライブ 1 0 2 において、メディアユニークキーおよびコンテンツキーを生成している。

レコーダを構成するドライブ 1 0 2 は、デバイスキー 1 2 1、プロセス M K B 1 2 2、C 2 \_\_ G 2 1 4 1、D E S (Data Encryption Standard) エンクリプタ 1 4 2、乱数発生器 1 4 3、C 2 \_\_ G 1 4 5、D  
15 E S エンクリプタ 1 4 6 の構成要素を有する。C 2 \_\_ G 2 1 4 1 は、メディア I D とメディアキーからメディアユニークキーを演算するブロックである。C 2 \_\_ G 2 1 4 5 は、タイトルキーと C C I 2 3 2 とからコンテンツキーを演算するブロックである。

メディア 1 0 1 から再生された M K B 1 1 2 とデバイスキー 1 2 1  
20 とがプロセス M K B 1 2 2 において演算されることによって、リボケーションされたかどうかの判別ができる。プロセス M K B 1 2 2 において、M K B 1 1 2 とデバイスキー 1 2 1 からメディアキーが算出される。M K B 1 1 2 の中にドライブ 1 0 2 のデバイスキー 1 2 1 が入っておらず、演算された結果が予め決められたある値例えばゼロの値  
25 と一致した場合、そのデバイスキー 1 2 1 を持つドライブ 1 0 2 が正当なものでないと判断され、ドライブ 1 0 2 がリボケーションされる

。

C 2 \_\_ G 1 4 1 は、メディアキーとメディア I D 1 1 1 とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーが D E S エンクリプタ 1 4 2 にてセッションキー K s によって暗号化される。暗号化の方式として、例えば D E S C B C モードが使用される。D E S エンクリプタ 1 4 2 の出力がホスト 1 0 3 の D E S デクリプタ 1 5 1 に送信される。

ドライブ 1 0 2 の乱数発生器 1 4 3 によってタイトルキーが生成され、乱数発生器 1 4 3 からのタイトルキーがホスト 1 0 3 の C 2 \_\_ E 1 5 3 に供給され、タイトルキーがメディアユニークキーを使用して C 2 によって暗号化される。暗号化タイトルキー 1 1 4 がメディア 1 0 1 に記録される。

ホスト 1 0 3 において、セッションキー K s を鍵として M A C 演算ブロック 1 5 8 により C C I の M A C 値 e K s ( C C I ) が計算され、C C I 2 3 2 とともにドライブ 1 0 2 へ転送される。

ドライブ 1 0 2 において、ホスト 1 0 3 から受け取った C C I 2 3 2 からセッションキー K s を鍵として M A C 演算ブロック 1 5 7 により C C I の M A C 値 e K s ( C C I ) が計算され、ホスト 1 0 3 から受け取った M A C 値とともに比較 1 5 9 へ供給される。

比較 1 5 9 では、両方の M A C 値が一致したならば、ホスト 1 0 3 から受け取った C C I 2 3 2 の改ざんは無いものと判断し、スイッチ S W 2 を O N する。一致しなかった場合は、C C I は改ざんされたものとみなし、スイッチ S W 2 を O F F し、以降の処理を中断する。

ドライブ 1 0 2 において、ホスト 1 0 3 から受け取った C C I 2 3 2 とタイトルキーとが C 2 \_\_ G 1 4 5 に供給され、コンテンツキーが導出される。コンテンツキーが D E S エンクリプタ 1 4 6 に供給され

、セッションキーK<sub>s</sub>を鍵として、コンテンツキーが暗号化される。  
暗号化コンテンツキーがホスト103のDESデクリプタ156に転送される。

5      ホスト103のDESデクリプタ156でセッションキーK<sub>s</sub>を鍵として復号されたコンテンツキーがC2\_\_ECBC155に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ113がドライブ102に転送され、ドライブ102によってメディア101に記録される。

第9図は、レコーダの一実施形態によるコンテンツ記録時の手順を示すものである。最初に、ホスト103からの要求に応じてメディア101上のMKBがシークされ、読み出される（ステップS61）。次のステップS62のAKE (Authentication and Key Exchange) において、上述したようなリボーク処理とドライブ102とホスト103の相互認証動作がなされる。

15      相互認証動作は、電源のON後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

20      相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ102およびホスト103の両者において、セッションキーK<sub>s</sub>が生成され、セッションキーK<sub>s</sub>が共有される。

25      次のステップS63において、ホスト103がドライブ102に対してメディアユニークキーを要求する。ドライブ102は、メディア101のメディアIDをシークし（ステップS64）、メディアID



をメディア 101 から読み出す（ステップ S65）。ドライブ 102 は、メディアキーとメディア ID とを演算することによってメディアユニークキーを生成する。ステップ S66 において、メディアユニークキーがセッションキー K<sub>s</sub> によって暗号化され、暗号化されたメディアユニークキーがホスト 103 に転送される。

次に、ステップ S67 において、ホスト 103 がドライブ 102 に対してタイトルキーを要求する。ステップ S68 において、ドライブ 102 がタイトルキーをホスト 103 に転送する。ホスト 103 において、セッションキー K<sub>s</sub> によって、暗号化されたメディアユニークキーが復号される。そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。

また、ステップ S69 において、ホスト 103 がドライブ 102 に対して CCI 232 を送る。このとき、CCI 232 の改ざんを回避するために CCI 232 の認証データとして計算された MAC 値 eK<sub>s</sub> (CCI) を付加して転送する。ドライブ 102 において、CCI 232 の改ざんが無いことを確認後、タイトルキーと CCI 232 からコンテンツキーが生成され、コンテンツキーがセッションキー K<sub>s</sub> で暗号化される。ステップ S70 において、ホスト 103 がドライブ 102 に対してコンテンツキーを要求すると、ステップ S71 において、ドライブ 102 が暗号化されたコンテンツキーをホスト 103 に送る。

ホスト 103 は、暗号化コンテンツキーをセッションキー K<sub>s</sub> によって復号し、コンテンツキーを得る。コンテンツキーによってコンテンツが暗号化される。ステップ S72 において、ホスト 103 からドライブ 102 に対して、暗号化タイトルキー、暗号化コンテンツおよび CCI 232 が転送される。ステップ S73 において、ドライブ 1

0 2 によって、暗号化タイトルキー、暗号化コンテンツおよび C C I  
2 3 2 がメディア 1 0 1 に対して記録される。

5 上述した第 8 図に示す構成のレコーダは、ドライブ 1 0 2 において、真正乱数またはそれに近い乱数をハードウェア例えば L S I によって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。また、ドライブ 1 0 2 において、ハードウェア構成によってコンテンツキーを生成するので、著作権保護の実装を強力とすることができる。

次に、上述した相互認証を行うドライブ 1 0 2 とホスト 1 0 3 とを  
10 組み合わせて実現したプレーヤの一実施形態の構成を第 1 0 図に示す。一実施形態のプレーヤは、ドライブ 1 0 2 が計算したメディアユニークキーを相互認証によって生成したセッションキー K s を用いてセキュアにホスト 1 0 3 に転送し、ホスト 1 0 3 が暗号化タイトルキーをメディアユニークキーによって復号し、タイトルキーと C C I 1 1  
15 5 とから導出したコンテンツキーを用いてコンテンツを復号する構成とされている。

プレーヤを構成するドライブ 1 0 2 は、デバイスキー 1 2 1、プロセス M K B 1 2 2、C 2 \_ G 2 1 4 1、D E S エンクリプタ 1 4 2 の構成要素を有する。メディア 1 0 1 から再生された M K B 1 1 2 とデ  
20 バイスキー 1 2 1 とがプロセス M K B 1 2 2 において演算されることによって、リボケーションされたかどうかの判別ができる。プロセス M K B 1 2 2 において、M K B 1 1 2 とデバイスキー 1 2 1 からメディアキーが算出される。

C 2 \_ G 1 4 1 は、メディアキーとメディア I D 1 1 1 とを演算し  
25 、メディアユニークキーを導出する処理である。メディアユニークキーが D E S エンクリプタ 1 4 2 にてセッションキー K s によって暗号

化される。暗号化の方式として、例えばDES CBCモードが使用される。DESエンクリプタ142の出力がホスト103のDESデクリプタ151に送信される。

5 ホスト103において、DESデクリプタ151において、セッションキーKsによってメディアユニークキーが復号される。メディアユニークキーおよび暗号化タイトルキー114がC2\_D153に供給され、暗号化タイトルキーがメディアユニークキーを使用して復号される。復号されたタイトルキーとメディア101から再生されたCCI115がC2\_G154に供給され、コンテンツキーが導出される。  
10 めディア101から再生された暗号化コンテンツ113がC2デクリプタ155において、コンテンツキーによって復号され、コンテンツキーが得られる。

第11図は、コンテンツ再生時の手順を示すものである。最初に、ホスト103からの要求に応じてメディア101上のMKBがシーク  
15 され、読み出される（ステップS41）。MKBがパック毎に読み出される。次のステップS42のAKEにおいて、上述したようなりボーク処理と、ドライブ102とホスト103の相互認証動作がなされる。

相互認証が成功しないと、リジェクト処理によって例えば処理が中  
20 断する。相互認証が成功すると、ドライブ102およびホスト103の両者において、セッションキーKsが生成され、セッションキーKsが共有される。

次のステップS43において、ホスト103がドライブ102に対してメディアユニークキーを要求する。ドライブ102は、メディア  
25 101のメディアIDをシークし（ステップS44）、メディアIDをメディア101から読み出す（ステップS45）。ドライブ102

は、メディアキーとメディアIDとを演算することによってメディアユニークキーを生成する。ステップS46において、メディアユニークキーがセッションキーKsによって暗号化され、暗号化されたメディアユニークキーがホスト103に転送される。

- 5 次に、ステップS47において、ホスト103がドライブ102に対して、暗号化タイトルキー、CCIおよび暗号化コンテンツを要求する。ステップS48において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113をメディア101からリードする。ステップS49において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113を読み取る。そして、ステップS50において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113をホスト103に対して転送する。

- 15 ホスト103において、タイトルキーが復号され、タイトルキーとCCI115とからコンテンツキーが求められ、コンテンツキーを鍵として暗号化コンテンツが復号される。

- 第10図に示すプレーヤの構成においては、ホスト103が暗号化タイトルキーを復号するデクリプタC2\_\_D153を備えているが、ドライブ102が暗号化タイトルキーを復号するデクリプタを備えるようにしても良い。この場合、復号されたタイトルキーがホスト103のコンテンツキー生成用のC2\_\_G154に対してセキュアに転送される。または、ドライブ102にコンテンツキー生成装置C2\_\_Gを設け、ドライブ102において復号されたタイトルキーとCCIとからコンテンツキーを生成するようにしても良い。この場合、復号されたコンテンツキーがホスト103のC2\_\_DCBC155へセキュアに転送される。

この発明のレコーダおよびプレイヤの他の実施形態について、第 1 2 図および第 1 3 図を参照して説明する。他の実施形態は、メディアユニークキーをドライブで生成するものであり、コンテンツキーを生成する場合に関与するパラメータを使用するもの（C P R M を拡張したシステム）である。

C P R M を拡張したシステムにおいて、メディアユニークキーを演算するためのパラメータ A と、暗号化／復号のためのパラメータ B とが使用される。これらのパラメータ A, B がホスト側にある場合と、ドライブ側にある場合と、メディアに記録されており、ホストが読み出す場合との全てが可能である。パラメータ A, B をインターフェースを介して授受する場合には、暗号化を行い、セキュアに伝送しても良い。

第 1 2 図は、レコーダの他の実施形態の構成を示す。第 1 2 図において、参照符号 2 0 1 が記録可能なメディアを示し、メディア 2 0 1 には、E K B 2 1 1、暗号化ディスクキー E m ( K d ) 2 1 2、ディスク I D 2 1 3 およびユニットキー生成用値 V u 2 1 4 が記録されている。

第 1 2 図中に記載されている鍵情報に関する用語を下記に説明する。

20 E K B 2 1 1 は、各デバイスキーに対してメディアキー K m を配布するための鍵束である。既述の実施形態におけるメディアキーブロック M K B に相当する。

メディアキー K m は、メディア毎に固有の鍵情報である。E K B の中にメディアキーが見つからない場合は、そのデバイスキーがリボー  
25 クされたことを示す。

ディスクキー K d は、少なくともコンテンツ毎に異なる鍵情報であ

る。コンテンツのマスターディスク毎に異ならせても良い。暗号化ディスクキーEm (Kd) 212は、メディアキーKmでディスクキーKdを暗号化した暗号化鍵で、メディア201に記録されている。暗号化ディスクキーEm (Kd) 212は、ドライブ102において、  
5 個々のメディア毎に異なるエンベディッドキーKeを生成するために使用される。

ユニットキー生成用値Vu 214は、暗号化単位（暗号化ユニットと称する）ごとに定義することが可能なパラメータである。各暗号化ユニットは、複数のセクタデータから構成される。ユニットキー生成用値Vu 214は、ホスト103においてコンテンツを暗号化する暗号化鍵としてのユニットキーKuを生成するために使用される。  
10

ディスクID 213は、スタンパ毎に異なるIDである。一実施形態におけるメディアID 111に相当する。

エンベディッドキーKeは、個々のメディア毎に異なる鍵情報であり、一実施形態におけるメディアユニークキーに相当する。  
15

ドライブ102が持つデバイスキー221と、メディア201が持つEKB 211とに基づいてプロセスEKB 222によってメディアキーKmが得られる。メディアキーKmとメディア201が持つ暗号化ディスクキーEm (Kd) 212とに基づいてAES\_D 223においてディスクキーKdが復号される。ディスクキーKdとディスクID 213とに基づいてAES\_G 224においてエンベディッドキーKeが得られる。  
20

ユニットキーKuは、コンテンツを暗号化する鍵であり、エンベディッドキーKeとユニットキー生成用値Vuとコピー制御情報CCI 232とに基づいて得られる。ユニットキーKuは、上述の一実施形態におけるコンテンツキーに相当する。  
25

上述した他の実施形態のレコーダの動作について処理の流れにしたがって説明する。

最初にAKE 225および227による認証がなされる。認証が成功すると、セッションキーK<sub>s</sub>が生成される。第12図では省略されているが、AKE 225および227の少なくとも一方に対して認証  
5 に関するパラメータが供給されている。

ドライブ102は、メディア201からEKB 211を読み出す。メディア201からのEKB 211とデバイスキー221がドライブ102のプロセスEKB 222で演算され、メディアキーK<sub>m</sub>が算出  
10 される。演算結果が例えば0になるような場合では、デバイスキーがリボークされる。ドライブ102が有しているデバイスキー221は、例えば機種単位でドライブに与えられる固有の鍵である。

ドライブ102が暗号化ディスクキーEm(K<sub>d</sub>) 212をメディア201から読み出し、AES\_\_D 223において、メディアキーK<sub>m</sub>によってディスクキーK<sub>d</sub>が得られる。AES(Advanced Encryption Standard)は、米国政府がDESに代わる新しい暗号化標準として  
15 採用した暗号化方法である。

さらに、ドライブ102は、メディア201からディスクID 213を読み出し、AES\_\_G 224において、ディスクIDとディスク  
20 キーK<sub>d</sub>を演算し、エンベディッドキーK<sub>e</sub>を得る。

ドライブ102とホスト103の認証が完了し、セッションキーK<sub>s</sub>が得られているならば、ホスト103がドライブ102に対してエンベディッドキーK<sub>e</sub>の転送を要求する。

ドライブ102がインターフェース104を経由してホスト103  
25 に対してK<sub>e</sub>を転送する際に、AESエンクリプタ226にてセッションキーK<sub>s</sub>によりK<sub>e</sub>を暗号化する。ホスト103は、AESデク

リプタ 2 2 8 によって復号を行い、K e を得る。A E S エンクリプタ 2 2 6 および A E S デクリプタ 2 2 8 は、例えば C B C (Cipher Block Chaining) モードの処理を行う。

5    ホスト 1 0 3 は、コンテンツを暗号化ユニット単位で処理する。ホスト 1 0 3 は、暗号化ユニットのユニットキー生成用値 V u 2 1 4 をドライブ 1 0 2 から読み出す。A E S \_ G 2 2 9 において、エンベディッドキー K e とユニットキー生成用値 V u 2 1 4 と C C I 2 3 2 とからユニットキー K u が計算される。ユニットキー K u の生成に C C I 2 3 2 を用いることで、コンテンツの著作権がより強固に保護される。  
10

ホスト 1 0 3 は、暗号化モジュール 2 3 0 において、コンテンツをユニットキー K u で暗号化する。暗号化コンテンツ 1 1 3 がドライブ 1 0 2 へ伝送され、記録可能なメディア 2 0 1 に記録される。

次に、第 1 3 図を参照してこの発明の他の実施形態のプレイヤについて説明する。プレイヤは、R O M タイプのメディア 2 1 0 例えば R O M ディスクを再生する例である。  
15

R O M タイプのメディア 2 1 0 には、予めコンテンツが記録されている。ホスト 1 0 3 では、暗号化の処理が不要となり、復号モジュール 2 3 1 が使用される。メディア 2 1 0 から読み出された暗号化コンテンツが復号モジュール 2 3 1 にて復号され、A V コンテンツが得られる。  
20

R O M タイプのメディア 2 1 0 の場合では、メディアキー K m およびディスクキー K d がコンテンツ毎に固有の鍵情報である。各コンテンツは、1 または複数の暗号化ユニットから構成される。

25    メディア 2 1 0 上にエンベディッドキー生成値 V e 2 1 5 が記録されている。エンベディッドキー生成値 V e 2 1 5 は、ディスク製造工



場でスタンパー（フォトレジストを現像したディスク原盤またはディスク原盤から最初に作成されたスタンパーを意味する）毎に、記録されたゼロでない値である。物理的ウォーターマークとして、通常のデータ記録とは、別の手段でディスク上に記録される。

- 5     エンベディッドキー  $K_e$  は、一実施形態におけるメディアユニークキーに相当する。エンベディッドキー  $K_e$  を生成するためのエンベディッドキー生成値  $V_e$  215 は、一種のメディア ID である。

- 第13図のレコーダは、第12図に示すプレイヤと同様の処理を行う。最初に  $AKE$  225 および 227 による認証がなされ、セッションキー  $K_s$  が生成される。読み出された  $EKB$  211 とデバイスキー 221 がドライブ 102 のプロセス  $EKB$  222 で演算され、メディアキー  $K_m$  が算出とリボーク処理がなされる。そして、 $AES\_D$  223 において、メディアキー  $K_m$  によってディスクキー  $K_d$  が復号される。さらに、 $AES\_G$  224 において、エンベディッドキー  $K_e$  15 が得られる。

$AES$  エンクリプタ 226 にてセッションキー  $K_s$  により  $K_e$  が暗号化される。ホスト 103 は、 $AES$  デクリプタ 228 によって復号を行い、 $K_e$  を得る。

- ホスト 103 は、読み出したい暗号化ユニットのユニットキー生成用値  $V_u$  214 およびコピー制御情報  $CCI$  をドライブ 102 から読み出し、 $AES\_G$  229 において、ユニットキー  $K_u$  が計算される。  
。

- ホスト 103 が要求した暗号化ユニットのセクタデータがホスト 103 の復号モジュール 231 において、属する暗号化ユニットのユニットキー  $K_u$  で復号される。  
25

この発明では、著作権保護技術に関する秘密情報である電子機器ま

たはアプリケーションソフトウェア固有の情報例えばデバイスキーが記録再生装置内に実装されているので、DVD処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報を持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

電子機器またはアプリケーションソフトウェア固有の情報としてのデバイスキーを記録再生装置とデータ処理装置が分けて持つことによって、記録再生装置およびアプリケーションソフトウェアの両方について、リボーク処理を行うことが可能となる。

この発明では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算が記録再生装置内に実装されている。したがって、データ処理装置のアプリケーションソフトウェアは、著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばタイトルキーは、タイトル毎のキーであるが、この発明では、乱数情報であれば、タイトル毎に異なることは、必要ではない。

また、上述した説明においては、著作権保護技術としてCPRMおよびCPRMを拡張した例を挙げたが、CPRM以外の著作権保護技術に対してもこの発明を適用することができる。例えば、特開2001-352322号公報において提案されるツリー構造の鍵配布構成

に基づく著作権保護技術に対して適用可能である。また、P C ベースのシステムに対してこの発明が適用されるが、このことは、P C とドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

この発明では、再生装置側でコンテンツキーを生成し、コンテンツキーを情報処理装置へ送信し、情報処理装置側でコンテンツキーによってコンテンツを暗号化している。このように著作権保護のための鍵情報の生成を再生装置で行うので、ハードウェア構成でコンテンツキーを生成することが可能となり、耐タンパー性を高めることができる。また、再生装置において、乱数を生成し、乱数を中間鍵とするので、再生装置において、真正乱数またはそれに近い乱数をハードウェア例えば L S I によって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。このように、この発明では、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持たせることが容易に実施でき、また、ディスクからのデータとしてそのまま読み出された暗号化コンテンツが「D e C S S」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を防ぐことができることから、著作権保護技術の安全性を確保することができる。

また、電子機器固有の情報としてのデバイスキーを記録再生装置が

持つことによって、記録再生装置自身をリポークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばL S Iによって生成できるので、P C内でソフトウェアによって乱数を生成5 するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

## 請 求 の 範 囲

1. 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達部を介して相互認証接続される
- 5 情報処理装置とを備える信号処理システムであって、  
上記再生装置は、  
中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、  
上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第 1
- 10 の送信部と、  
上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第 2 の送信部とを有し、  
上記情報処理装置は、  
上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコ
- 15 ンテンツ情報暗号化部と、  
上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化部と、  
暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録部とを有する信号処理システム。
- 20 2. 請求の範囲 1 において、  
上記再生装置は、  
乱数を生成する乱数生成部を有し、  
上記中間鍵情報は、  
上記乱数生成部により生成された乱数である信号処理システム。
- 25 3. 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達部を介して相互認証接続される

情報処理装置とが、上記記録媒体に情報を記録する記録方法であって、  
上記再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

- 5    上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第 1 の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第 2 の送信ステップとを有し、

上記情報処理装置は、

- 10   上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

- 15   暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを有する記録方法。

4. 請求の範囲 3 において、

上記再生装置は、

乱数を生成する乱数生成ステップを有し、

- 20   上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数である記録方法。

5. 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達部を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録するプログラムであって、

- 25   て、

上記再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第1の送信ステップと、

- 5   上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第2の送信ステップとを行わせ、

上記情報処理装置に、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

- 10   上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを行わせるプログラム

15   。

6. 請求の範囲5において、

上記再生装置に、

乱数を生成する乱数生成ステップを行わせ、

上記中間鍵情報は、

- 20   上記乱数生成ステップにより生成された乱数であるプログラム。

7. 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達部を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録するプログラムを格納した記録媒体であって、

- 25   上記再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号

化鍵生成ステップと、

上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第 1  
の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装  
5 置へ送る第 2 の送信ステップを行わせ、

上記情報処理装置に、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコ  
ンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情  
10 報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと

、  
暗号化された上記コンテンツ情報および暗号化された上記中間鍵情  
報とを上記記録媒体に記録する記録ステップとを行わせるプログラム  
を格納した記録媒体。

15 8. 請求の範囲 7 において、

上記再生装置に、

乱数を生成する乱数生成ステップを行わせ、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数であるプログラムを格  
20 納した記録媒体。

9. 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み  
出し、伝達部を介して情報処理装置と接続される再生装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号  
化鍵生成部と、

25 上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第 1  
の送信部と、



上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第 2 の送信部とを有し、

- 上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化部と、暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録部とを有する上記情報処理装置と相互認証接続される再生装置。
- 5

1 0 . 請求の範囲 9 において、

- 10 乱数を生成する乱数生成部を有し、

上記中間鍵情報は、

上記乱数生成部により生成された乱数である再生装置。

1 1 . 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と伝達部を介して接続される情報処理装置であって、

- 15 中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第 1 の送信部と、上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第 2 の送信部とを有する上記再生装置と伝達部を介して相互認証接続され、

- 20 上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化部と、

- 暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報  
25 報を上記記録媒体に記録する記録部とを有する情報処理装置。

1 2 . 請求の範囲 1 1 において、

上記再生装置は、

乱数を生成する乱数生成部を有し、

上記中間鍵情報は、

上記乱数生成部により生成された乱数である情報処理装置。

5 1 3. 不正な電子機器を無効化するための第 1 の情報と、コンテンツ毎に異なる第 2 の情報と、暗号化単位毎に定義可能な第 3 の情報と、スタンパ毎に異なる識別データとが記録された記録媒体へ暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

10 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 4 の情報が格納される格納部と、

上記第 1 の情報と上記第 4 の情報とから当該格納された第 4 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報で

15 あるかを判定するリボーク処理部と、

上記リボーク処理部で上記第 4 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であると判定された場合に、上記第 1 の情報、上記第 4 の情報、上記第 2 の情報および上記識別データから、個々の記録媒体毎に固有の中間鍵情報を求める演算部と、

20 上記中間鍵情報を伝達部を介して情報処理装置の最終暗号化鍵生成部へ送る送信部とを有する再生装置。

1 4. 請求の範囲 1 3 において、

上記中間鍵情報に基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理

25 装置と相互認証を行う認証部と、

上記認証が成立した場合に形成されるセッションキーによって上記

中間鍵情報を暗号化して上記データ処理装置に送出する中間鍵情報暗号化部とを有する記録再生装置。

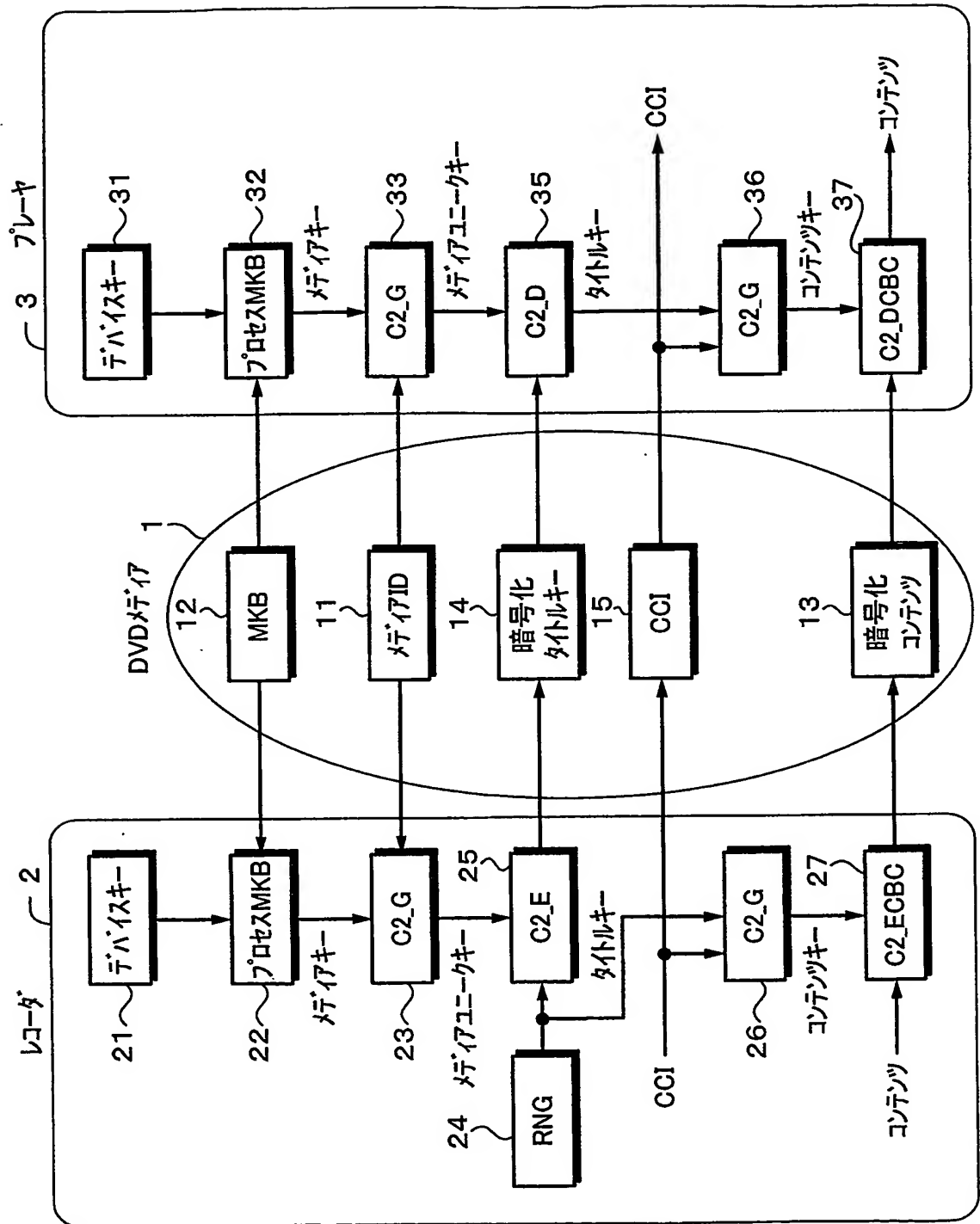
- 15 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 4 の情報を有するとともに、不正な電子機器を無効化するための第 1 の情報と、コンテンツ毎に異なる第 2 の情報と、暗号化単位毎に定義可能な第 3 の情報と、スタンプ毎に異なる識別データとが記録された記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置との認証を行う認証部と、

- 上記記録再生装置から、上記認証が成立した場合に形成されるセッションキーによって暗号化された、上記第 1 の情報、上記第 4 の情報、上記第 2 の情報および上記識別データから生成された個々の記録媒体毎に固有の中間鍵情報を受け取り、当該中間鍵情報を復号する鍵情報復号部と、

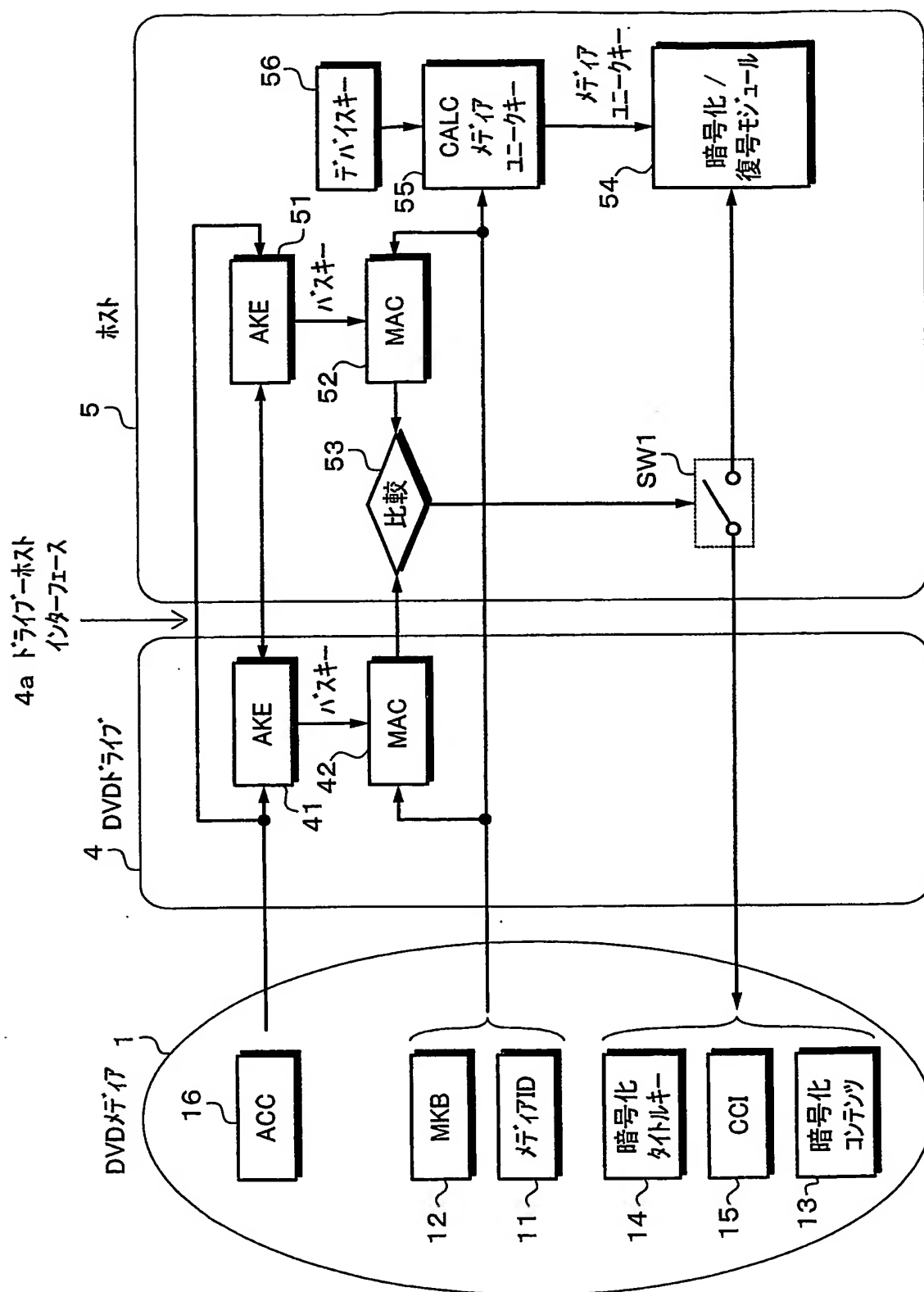
上記記録再生装置から受け取った上記第 3 の情報と、復号された上記中間鍵情報から最終暗号化鍵を生成する最終暗号化鍵生成部と、

上記最終暗号化鍵による暗号化と上記最終暗号化鍵による復号との少なくとも一方を行う暗号化復号部とを有するデータ処理装置。

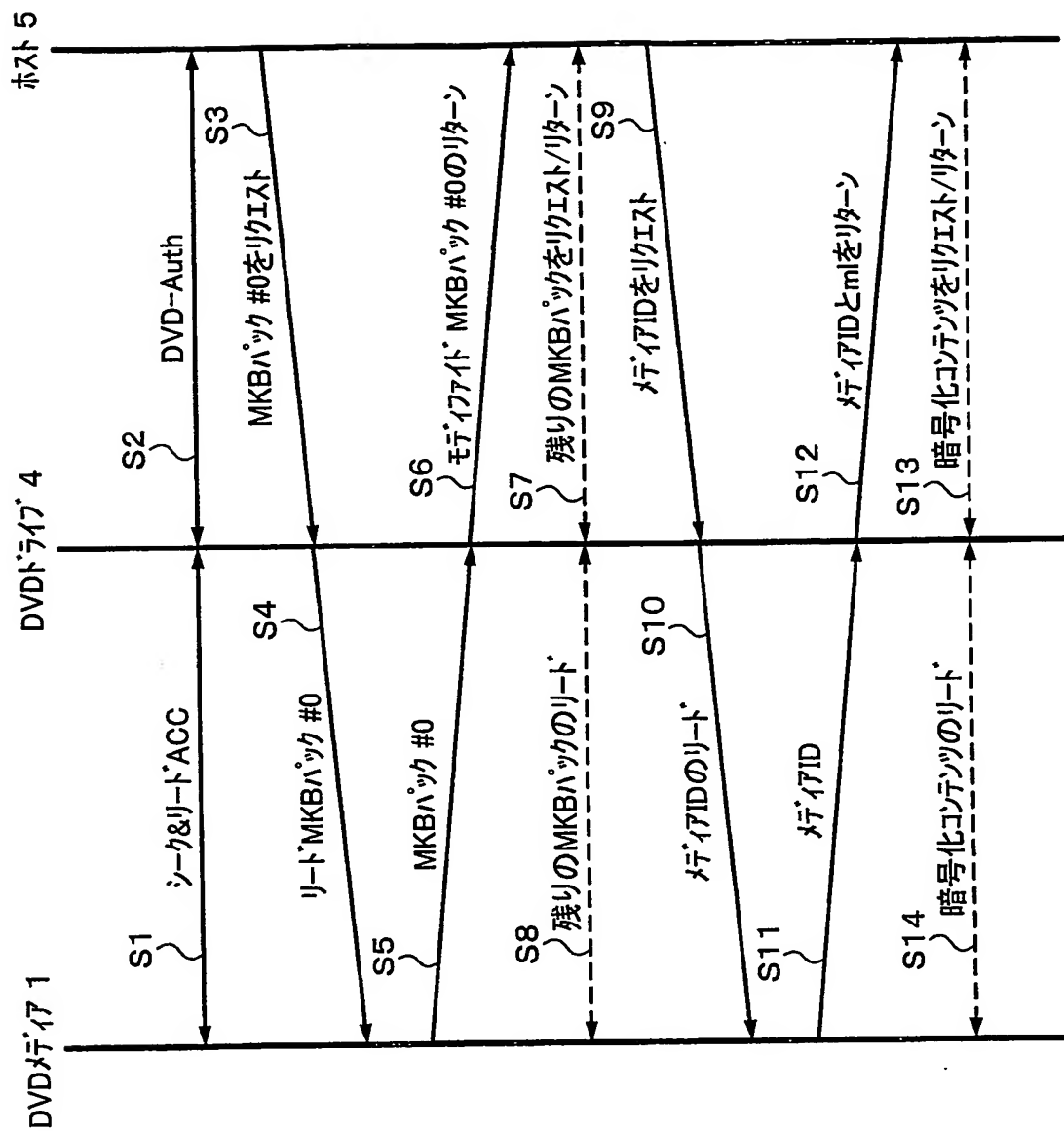
第1図



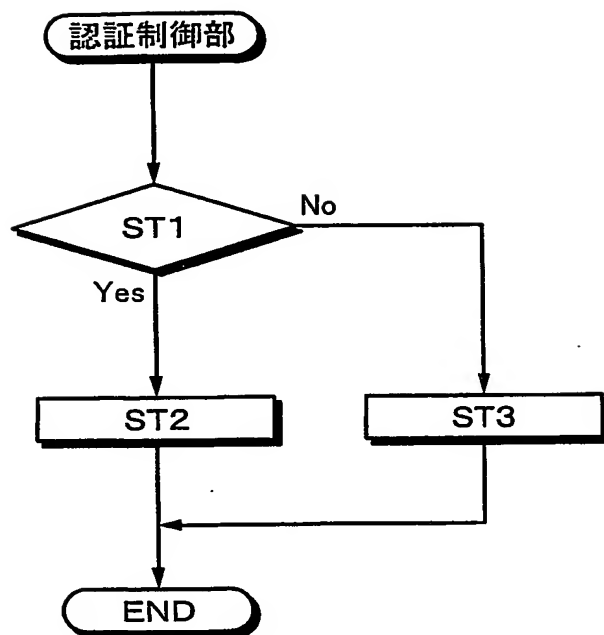
## 第2図



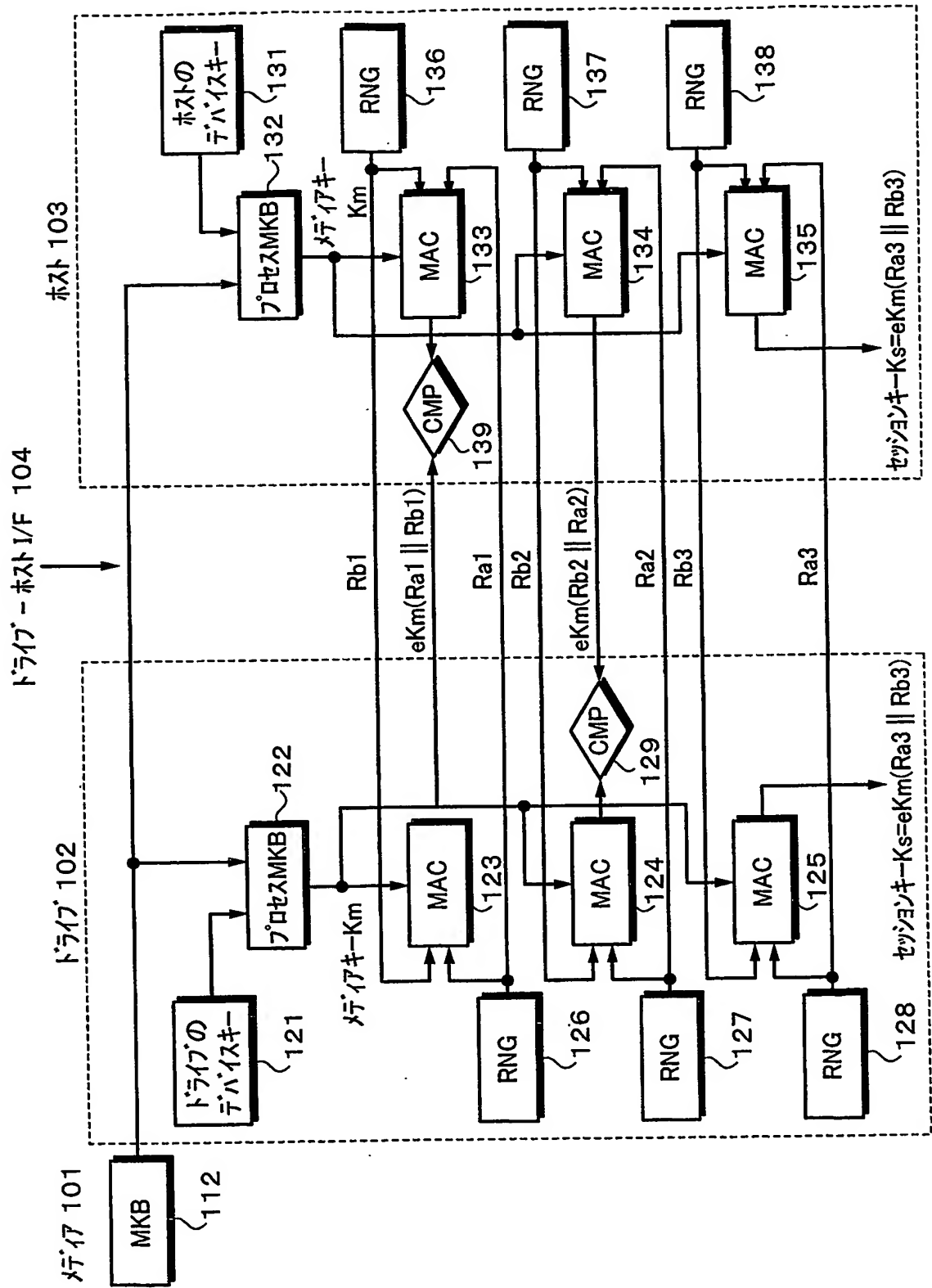
## 第3図



## 第4図



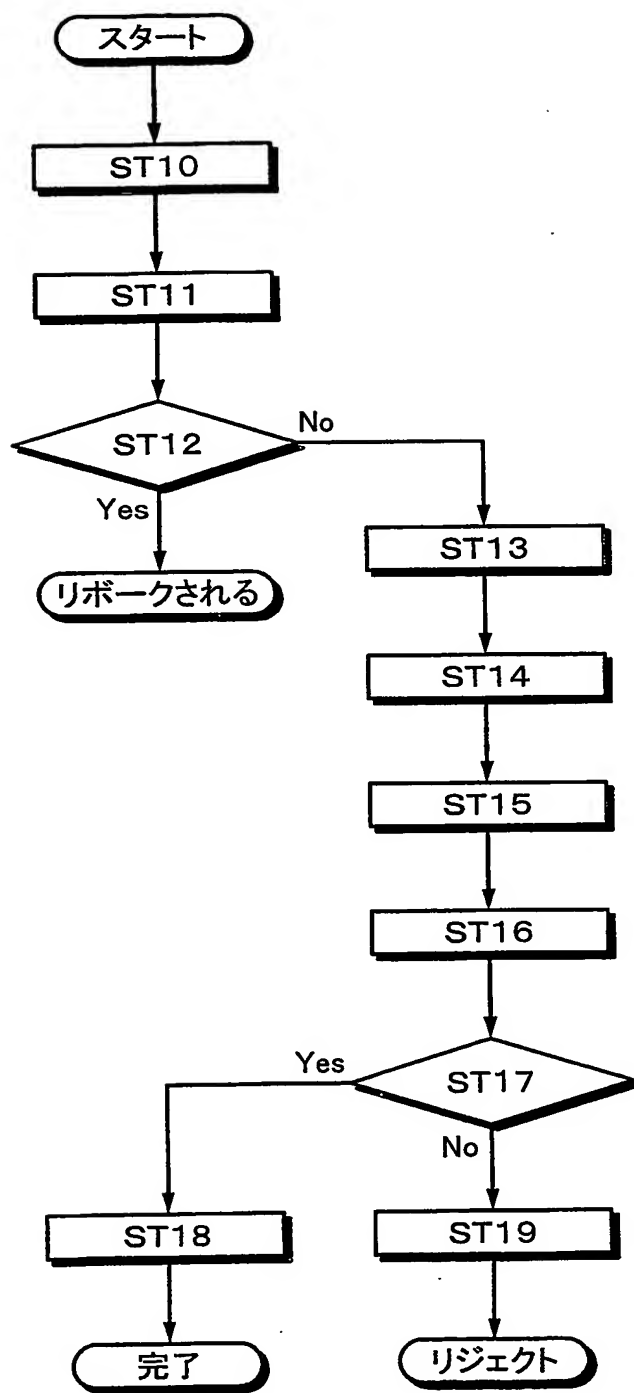
## 第5図



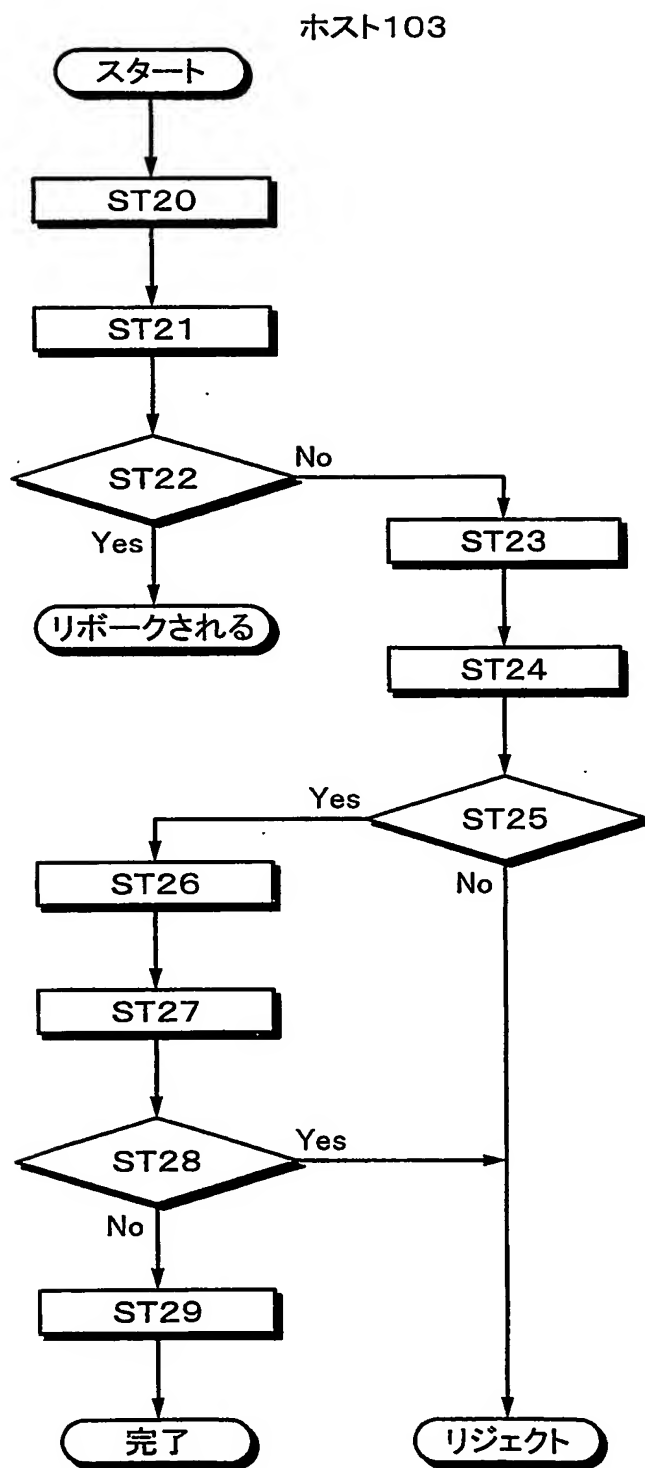


## 第6図

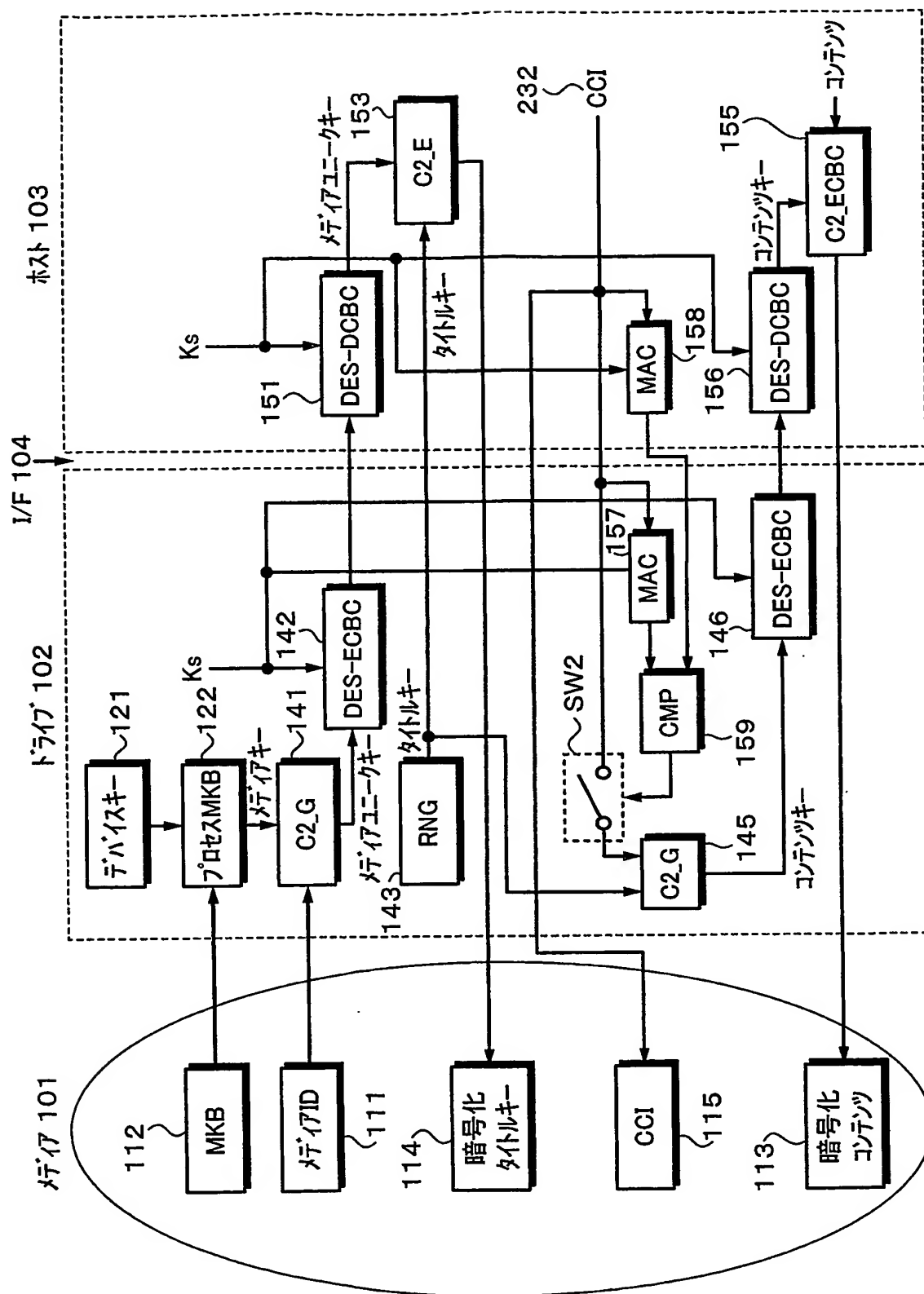
ドライブ102



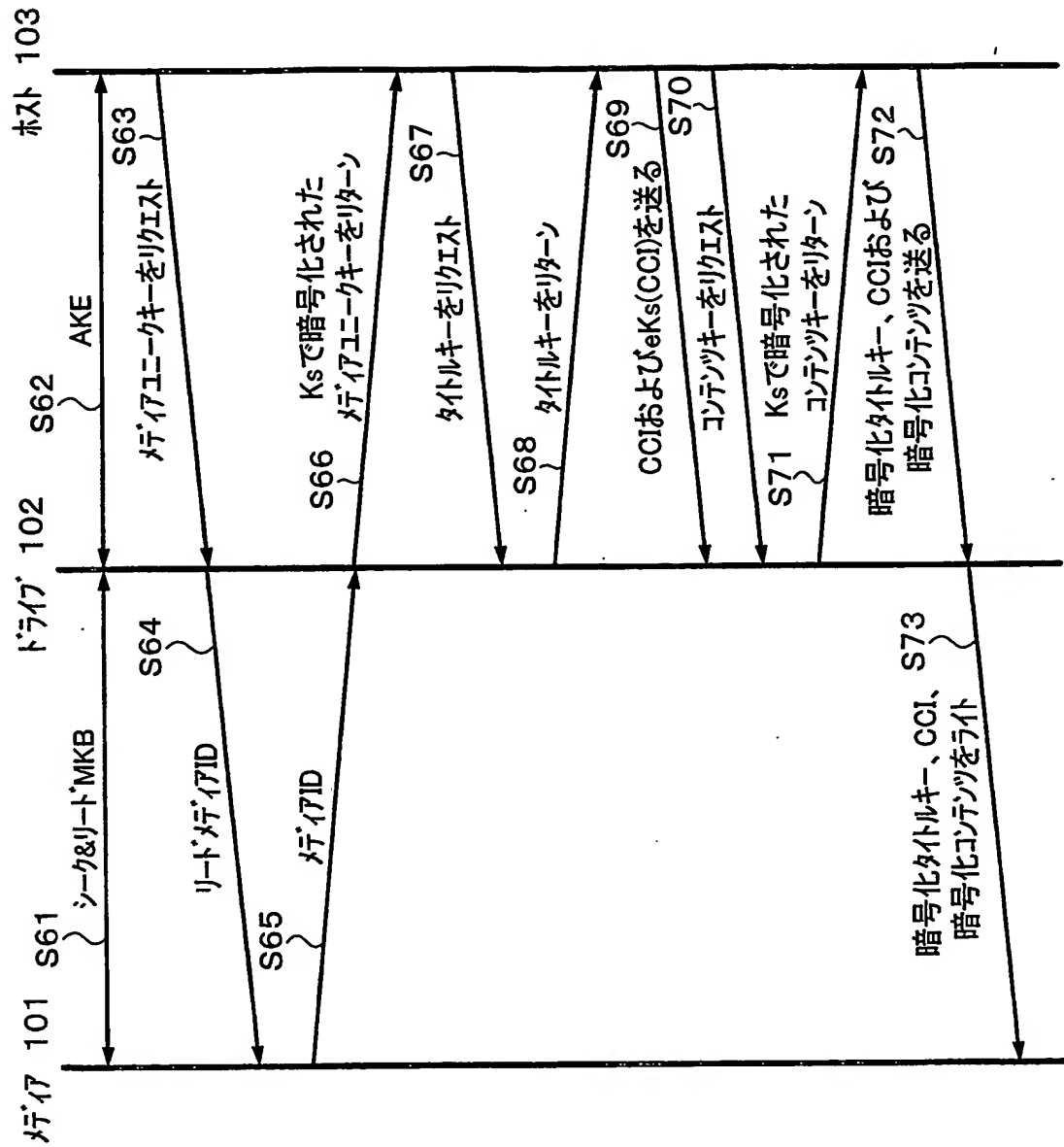
## 第7図



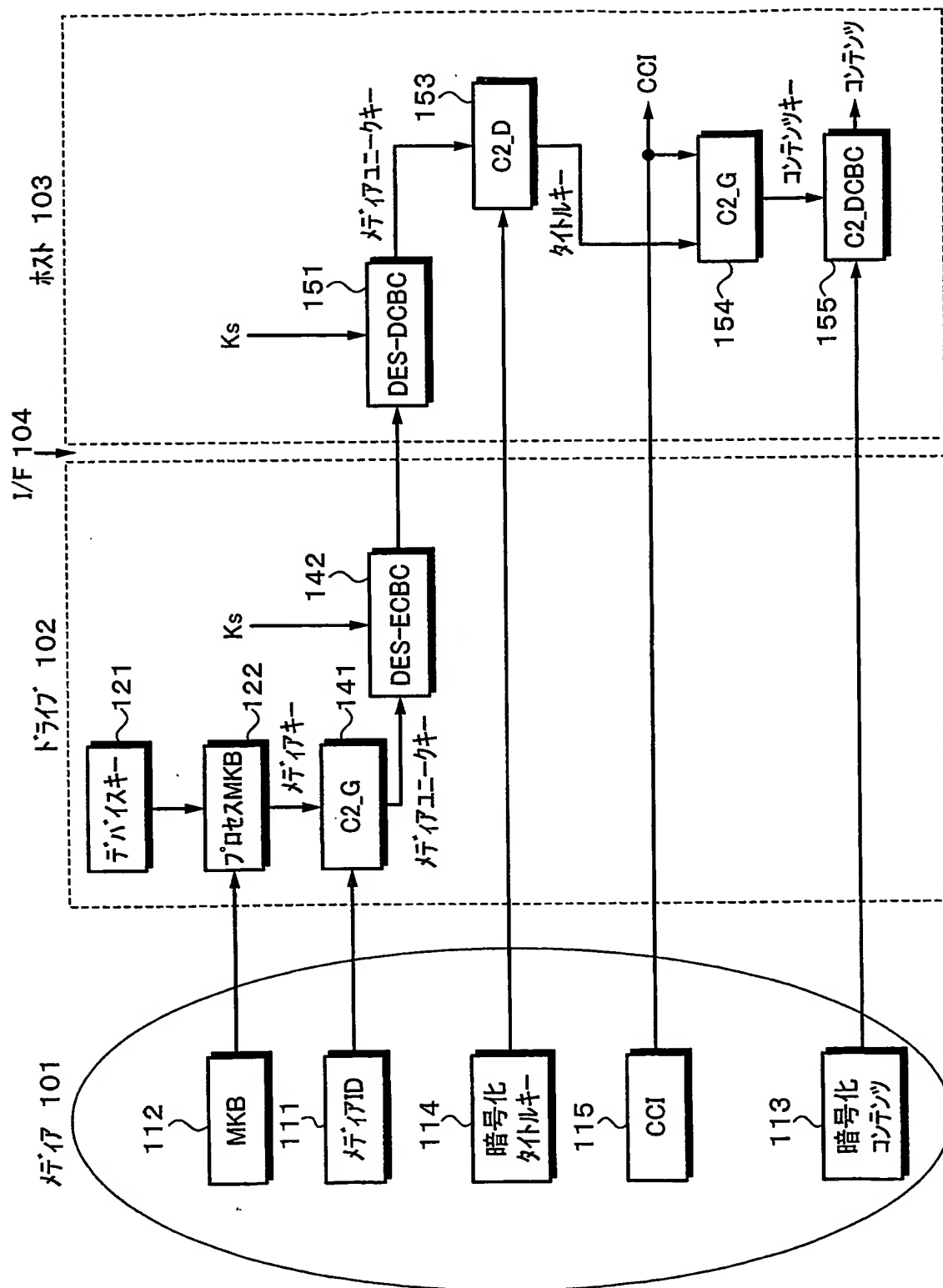
八  
 八  
 集



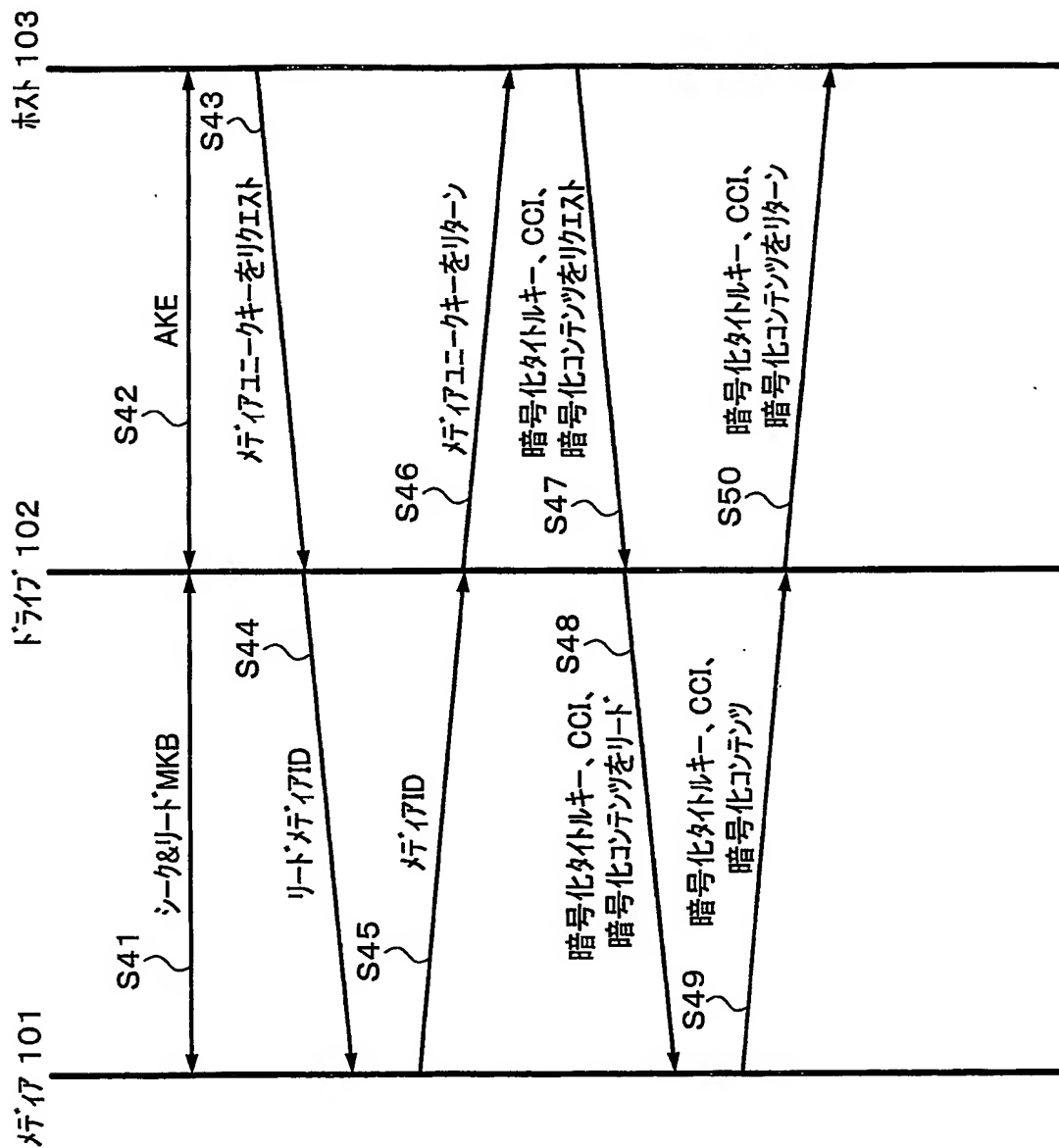
## 第9図



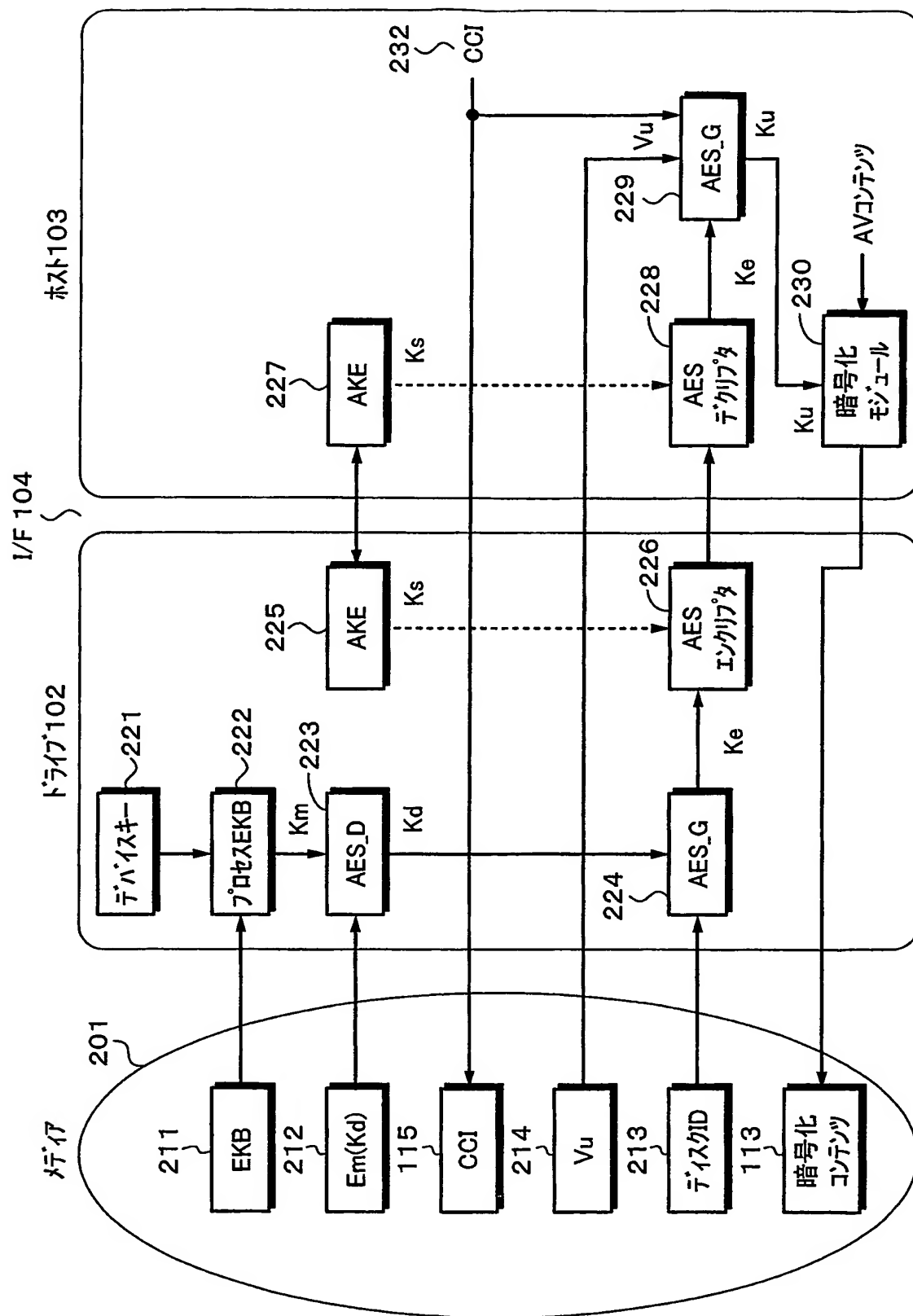
第10図



# 第11図



## 第12図







## 符号の説明

1	D V Dメディア
2	レコーダ
3	プレーヤ
4	D V Dドライブ
4 a	インターフェース
5	ホスト
1 1 1	メディア I D
1 1 2	メディアキーブロック (M K B)
1 1 3	暗号化コンテンツ
1 0 1	メディア
1 0 2	ドライブ
1 0 3	ホスト
1 0 4	インターフェース
1 2 1	ドライブのデバイスキー
1 2 2	プロセスM K B
1 2 3、1 2 4、1 2 5	ドライブのM A C演算ブロック
1 2 6、1 2 7、1 2 8	ドライブの乱数発生器
1 2 9	比較
1 3 1	ホストのデバイスキー
1 3 2	プロセスM K B
1 3 3、1 3 4、1 3 5	ホストのM A C演算ブロック
1 3 6、1 3 7、1 3 8	ホストの乱数発生器
1 3 9	比較
1 4 1、1 5 4	C 2 _ G

1 4 2、1 4 6     D E S エンクリプタ  
1 4 3     乱数発生器  
1 5 1、1 5 2、1 5 6     D E S デクリプタ  
1 5 3     C 2 \_\_ E  
1 5 5     C 2 \_\_ E B C  
1 5 7、1 5 8     M A C 演算ブロック  
1 5 9     比較  
S T 1     M A C 計算値が一致？  
S T 2     スイッチを O N  
S T 3     スイッチを O F F  
S T 1 0     R E P O R T   K E Y ( M K B )  
S T 1 1     メディアキー  $K_m$  を計算  
S T 1 2     リボーク？  
S T 1 3     R E C E I V E ( R b 1 , R b 2 )  
S T 1 4     R E T U R N (  $eK_m(Ra1 \parallel Rb1)$ , R a 1 )  
S T 1 5     R E T U R N ( R a 2 , R a 3 )  
S T 1 6     R E C E I V E  
(  $eK_m(Rb2 \parallel Ra2)$ , R b 3 )  
S T 1 7     同一の M A C ？  
S T 1 8     セッションキーの確定  
(  $eK_m(Ra3 \parallel Rb3)$  )  
S T 1 9     R E T U R N ( エラー )  
S T 2 0     R E P O R T   K E Y ( M K B )  
S T 2 1     メディアキー  $K_m$  を計算  
S T 2 2     リボーク？  
S T 2 3     S E N D   K E Y ( R b 1 , R b 2 )

ST 2 4      R E P O R T   K E Y  
                     $(eK_m(Ra1 \parallel Rb1), Ra1)$

ST 2 5      同一のMAC?

ST 2 6      R E P O R T   K E Y (Ra2, Ra3)

ST 2 7      S E N D   K E Y  
                     $(eK_m(Rb2 \parallel Ra2), Rb3)$

ST 2 8      エラー?

ST 2 9      セッションキーの確定  
                     $(eK_m(Ra3 \parallel Rb3))$

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/16937

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L9/10, G11B20/10, G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L9/10, G11B20/10, G11B20/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004  
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
WPI, DVD, media, cipher, encryption

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 9-190667 A (Toshiba Corp.), 22 July, 1997 (22.07.97), All pages & WO 97/25711 A1 & AU 9711099 A & EP 814474 A1 & TW 316301 A & KR 97706539 A & CA 2199241 C & JP 2001-292136 A & CN 1176014 A & US 6347846 B1 & US 2002/0061105 A1	1-15.
A	JP 11-66706 A (Toshiba Corp.), 09 March, 1999 (09.03.99), All pages (Family: none)	1-15
A	JP 2000-100069 A (Toshiba Corp.), 07 April, 2000 (07.04.00), All pages (Family: none)	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

\* Special categories of cited documents:  
"A" document defining the general state of the art which is not considered to be of particular relevance  
"E" earlier document but published on or after the international filing date  
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other means  
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
"&" document member of the same patent family

Date of the actual completion of the international search  
16 April, 2004 (16.04.04)

Date of mailing of the international search report  
27 April, 2004 (27.04.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## 国際調査報告

国際出願番号 PCT/JPO3/16937

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/10, G11B20/10, G11B20/12

## B. 調査を行った分野

## 調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/10, G11B20/10, G11B20/12

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

## 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI  
DVD, media, cipher, encryption

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 9-190667 A (株式会社東芝) 1997. 07. 22, 全頁を参照 & WO 97/25711 A1 & AU 9711099 A & EP 814474 A1 & TW 316301 A & KR 97706539 A & CA 2199241 C & JP 2001-292136 A & CN 1176014 A & US 6347846 B1 & US 2002/0061105 A1	1-15
A	JP 11-66706 A (株式会社東芝) 1999. 03. 09, 全頁を参照 (ファミリーなし)	1-15
A	JP 2000-100069 A (株式会社東芝) 2000. 04. 07, 全頁を参照 (ファミリーなし)	1-15

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に関する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

16. 04. 2004

国際調査報告の発送日

27. 4. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

9364

電話番号 03-3581-1101 内線 3597